

**DELETING COMMERCIAL  
PORNOGRAPHY SITES FROM THE  
INTERNET: THE U.S. FINANCIAL  
INDUSTRY'S EFFORTS TO COMBAT  
THIS PROBLEM**

---

HEARING  
BEFORE THE  
SUBCOMMITTEE ON OVERSIGHT AND  
INVESTIGATIONS  
OF THE  
COMMITTEE ON ENERGY AND  
COMMERCE  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED NINTH CONGRESS  
SECOND SESSION

SEPTEMBER 21, 2006

**Serial No. 109-141**

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

31-467PDF

WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas	JOHN D. DINGELL, Michigan
MICHAEL BILIRAKIS, Florida	<i>Ranking Member</i>
<i>Vice Chairman</i>	HENRY A. WAXMAN, California
FRED UPTON, Michigan	EDWARD J. MARKEY, Massachusetts
CLIFF STEARNS, Florida	RICK BOUCHER, Virginia
PAUL E. GILLMOR, Ohio	EDOLPHUS TOWNS, New York
NATHAN DEAL, Georgia	FRANK PALLONE, JR., New Jersey
ED WHITFIELD, Kentucky	SHERROD BROWN, Ohio
CHARLIE NORWOOD, Georgia	BART GORDON, Tennessee
BARBARA CUBIN, Wyoming	BOBBY L. RUSH, Illinois
JOHN SHIMKUS, Illinois	ANNA G. ESHOO, California
HEATHER WILSON, New Mexico	BART STUPAK, Michigan
JOHN B. SHADEGG, Arizona	ELIOT L. ENGEL, New York
CHARLES W. "CHIP" PICKERING, Mississippi	ALBERT R. WYNN, Maryland
<i>Vice Chairman</i>	GENE GREEN, Texas
VITO FOSSELLA, New York	TED STRICKLAND, Ohio
ROY BLUNT, Missouri	DIANA DEGETTE, Colorado
STEVE BUYER, Indiana	LOIS CAPPS, California
GEORGE RADANOVICH, California	MIKE DOYLE, Pennsylvania
CHARLES F. BASS, New Hampshire	TOM ALLEN, Maine
JOSEPH R. PITTS, Pennsylvania	JIM DAVIS, Florida
MARY BONO, California	JAN SCHAKOWSKY, Illinois
GREG WALDEN, Oregon	HILDA L. SOLIS, California
LEE TERRY, Nebraska	CHARLES A. GONZALEZ, Texas
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MIKE ROGERS, Michigan	TAMMY BALDWIN, Wisconsin
C.L. "BUTCH" OTTER, Idaho	MIKE ROSS, Arkansas
SUE MYRICK, North Carolina	
JOHN SULLIVAN, Oklahoma	
TIM MURPHY, Pennsylvania	
MICHAEL C. BURGESS, Texas	
MARSHA BLACKBURN, Tennessee	

BUD ALBRIGHT, *Staff Director*

DAVID CAVICKE, *General Counsel*

REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

ED WHITFIELD, Kentucky, *Chairman*

CLIFF STEARNS, Florida	BART STUPAK, Michigan
CHARLES W. "CHIP" PICKERING, Mississippi	<i>Ranking Member</i>
CHARLES F. BASS, New Hampshire	DIANA DEGETTE, Colorado
GREG WALDEN, Oregon	JAN SCHAKOWSKY, Illinois
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MICHAEL C. BURGESS, Texas	TAMMY BALDWIN, Wisconsin
MARSHA BLACKBURN, Tennessee	HENRY A. WAXMAN, California
JOE BARTON, Texas	JOHN D. DINGELL, Michigan
<i>(EX OFFICIO)</i>	<i>(EX OFFICIO)</i>

# CONTENTS

---

	Page
Testimony of:	
Christie, Hon. Christopher J., United States Attorney, District of New Jersey, U.S. Department of Justice.....	17
Allen, Ernie, President and Chief Executive Officer, National Center for Missing and Exploited Children .....	28
Plitt, James, Director, Cyber Crimes Center, Office of Investigations, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security .....	33
Christenson, Arne L., Senior Vice President, Federal Government Affairs, American Express Company.....	51
Golinsky, Jodi, Vice President and Senior Regulatory Counsel, MasterCard International, Inc. ....	60
Sullivan, Joe, Associate General Counsel, PayPal, Inc. ....	66
McCarthy, Mark, Senior Vice President, Public Policy, VISA U.S.A., Inc. ....	70
Jackson, Dr. Douglas, Chairman, e-gold Group, Inc. ....	73
Matos, William, Senior Director, Credit/Risk, Chase Paymentech Solutions, L.L.C. ....	103
Mowder, Senior Vice President, Bank of America .....	109
Shalom, Ralph, Associate General Counsel for Litigation, First Data Corporation .....	115
Strider, David, Executive Vice President, North American Operations, NOVA Information Systems, U.S. Bancorp .....	120



# **DELETING COMMERCIAL PORNOGRAPHY SITES FROM THE INTERNET: THE U.S. FINANCIAL INDUSTRY'S EFFORTS TO COMBAT THIS PROBLEM**

**THURSDAY, SEPTEMBER 21, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Whitfield, Stearns, Pickering, Ferguson, Burgess, Blackburn, Barton (ex officio), Stupak, DeGette, and Inslee.

Staff Present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Kelli Andrews, Counsel; Karen Christian, Counsel; John Halliwell, Policy Coordinator; Ryan Ambrose, Legislative Clerk; David Nelson, Minority Investigator; Jonathon Brater, Minority Staff Assistant; and Elizabeth Ertel, Minority Senior Staff Assistant.

MR. WHITFIELD. I would like to call this hearing to order this morning, and today the subcommittee will hold its sixth hearing to explore issues relating to the sexual exploitation of children over the Internet. I must say for all of us, we have all really been appalled at how widespread this problem is, not only in America but around the world. We have learned a lot about this pervasive problem and the ways in law enforcement and industry can and should work together to eradicate sites that continue to victimize children and put perpetrators behind bars.

I would like to highlight several important issues that have been raised through our hearings. First, Federal, State, and local law enforcement need more resources to combat these crimes due to the technological expertise required to catch online pedophiles and the increasing number of pedophiles that are using the Internet as a way to victimize children. This July Congress passed and President Bush signed into law the Adam Walsh Act of 2006, which in addition to establishing a national sex offender registry also authorizes additional law

enforcement officers and other resources specifically for combating sexual crimes against children, and we all support that effort.

Second, we learned that Internet service providers and social networking sites have information that law enforcement needs when investigating pedophiles online, and that is the IP address on a particular date and time that will help identify those involved. There is disparity among the Internet providers on the length of time they retain IP address data. Several members of the industry have agreed to lengthen their data retention time for this particular data, and we are all pleased with their efforts.

Tuesday a week ago, Attorney General Gonzalez testified before the Senate that the Department of Justice is supportive of legislation mandating a 2-year retention policy for IP address information and investigations involving the sexual exploitation of children. I would say that most of the members of our panel probably support that recommendation. Finally, through Marsha Allen and Justin Berry, two victims of child predators, whose images were repeatedly sold and traded over the Internet by these pedophiles, and we know the images of their sexual abuse that are now on the Internet will be there forever, we must work aggressively to put the child pornographers out of business.

Today we address another critical component to combating the sexual exploitation of children over the Internet, the financial industry's role in shutting down commercial child pornography sites. This is a multi-billion dollar illicit industry. This business does not just involve the people that post the sexually exploitive images of the children, but it also involves a credit card processing company for the site. We will hear testimony today from the United States Attorney for New Jersey, Chris Christie, who will tell us about the RegPay case that his office successfully prosecuted.

The RegPay case involved a commercial child pornography site based out of Russia and a credit card processing company in the U.S. We will also hear from Ernie Allen about the financial coalition that was formed as an alliance between the National Center, some members of the financial industry, the Internet service providers, and law enforcement and how this coalition is working to shut down commercial child pornography sites. Immigration and Customs representatives will testify today about trends they are seeing in the payment world as it relates to commercial child pornography.

We will also hear about digital currency in lieu of credit cards, and how that is being used as an alternate method of payment. These methods of payments make it impossible to track the purchaser or the merchant and are ripe for abuse by criminals and are being used to foster crimes including exploiting children online. We had hoped to hear a

John Doe witness today who was going to be testifying from a Federal penitentiary and how he became involved with a group from overseas and he was processing their credit card payments. He is in a Federal prison, but due to some legal issues and others, we are not going to have his testimony.

I will tell you though that he was netting over \$300,000 a month in revenue from processing these subscriptions to the websites, and the Web masters of the child pornography sites, as I said, all outside the jurisdiction of the U.S., were clearing much more than that. And we are sorry that he will not be able to testify. On the third and fourth panels, we will hear from the payment industry, the acquiring banks, and the merchant processing companies. The first question that many of us have is why can't the credit card company just shut a site down once it finds out it contains sexually exploitive images of children.

Now we know that many steps have been taken by the processing companies and we commend them on that, but we want to urge them to do more. And only with continued collaboration among industry, law enforcement, and the National Center will these commercial sites be deleted from the Internet once and for all. I want to thank all the witnesses, and we will be introducing the panels a little bit later. At this time I would like to recognize the Ranking Member, Mr. Stupak of Michigan.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

Good Morning. Today the Subcommittee will hold its sixth hearing to explore issues relating to the sexual exploitation of children over the Internet worldwide. We have learned a lot about this pervasive problem and the ways in which law enforcement and industry can and should work together to eradicate sites that continue to victimize children and put perpetrators behind bars. I'd like to highlight several important issues that have been raised through our hearings:

First, Federal, state and local law enforcement need more resources to combat these crimes due to the technological expertise required to catch online pedophiles and the increasing number of pedophiles that are using the internet as to victimize children. This July, Congress passed, and President Bush signed into law, The Adam Walsh Act of 2006, which in addition to establishing a national sex offender registry also authorizes additional law enforcement officers and other resources specifically for combating sexual crimes against children.

Second, we learned that Internet Service Providers and social networking sites have information that law enforcement needs when investigating pedophiles on-line--the "IP Address" on a particular date and time that will help identify those involved. There is disparity among Internet providers on the length of time they retain IP address data. Several members of the industry have agreed to lengthen their data retention time for this particular data and I am pleased with their efforts. Tuesday a week ago, Attorney General Gonzales testified before the Senate that the Department of Justice is supportive of

legislation mandating a two-year data retention policy for IP address information in investigations involving the sexual exploitation of children.

Finally, through Masha Allen and Justin Berry-two victims of child predators whose images were repeatedly sold and traded over the Internet by these pedophiles. We have the images of their sexual abuse that are now on the Internet and will be there forever. We must work aggressively to put the child pornographers out of business. It is for all the children whose images are on the Internet that we must work tirelessly to identify those victims and save them and to send this child pornography industry into the gutter, where it belongs.

Today we address another critical component to combating the sexual exploitation of children over the Internet: the financial industry's role in shutting down commercial child pornography sites. This is a multi-billion dollar illicit industry. This business does not just involve the people that post the sexually exploitative images of the children but it also involves a credit card processing company for the site. We will hear testimony today from the United States Attorney for New Jersey, Chris Christie, who will tell us about the Regpay case that his office successfully prosecuted. The Regpay case involved a commercial child pornography site based out of Russia, and the credit card processing company was in the U.S. We will also hear from Ernie Allen about the Financial Coalition that was formed as an alliance between the National Center, some members of the financial industry, the internet service providers and law enforcement and how this coalition is working to shut down commercial child pornography sites. Immigration and Customs Enforcement reps will testify about trends they are seeing in the payment world as it relates to commercial child pornography sites. We will also hear about digital currency in lieu of credit cards and how it is being used as an alternate method of payment. These methods of payments make it impossible to track the purchaser or the merchant and are ripe for abuse by criminals and are being used to foster crimes, including exploiting children on-line.

We hoped to hear a John Doe witness today who was going to be testifying from a federal penitentiary and how he became involved with a group overseas and he was processing their credit card payments. He is in federal prison but due to some legal issues and other we will not have his testimony. He is currently serving a lengthy federal sentence for these crimes. I will tell you that he was netting over \$300K a month in revenue from processing subscriptions to these websites and the webmasters of the child pornography sites who are outside the jurisdiction of the United States are earning far more. We are sorry he will not be able to testify.

On the third and fourth panels, we will hear from the payment industry, the acquiring banks and the merchant processing companies. The first question that many of us have is--why can't the credit card company just shut a site down once it finds out it contains sexually exploitative images of children? I applaud the industry for all of the proactive measures they are taking to eradicate commercial child pornography sites from the Internet and I urge them to continue to do more. Only with the continued collaboration among industry, law enforcement and the National Center will these commercial sites be deleted from the Internet once and for all.

I thank all of the witnesses for being here today and conclude my opening statement.

MR. STUPAK. Thank you, Mr. Chairman. As you said, this is our sixth hearing on the scourge of child pornography. The problem of child pornography is of great concern to all Members of Congress, Democrats, Republicans, Independents. Until recently this committee's hearings have been bipartisan. Today's hearing includes repeat testimony of the August hearing in New Jersey. This testimony is being repeated today



for political and not meritorious reasons. For the record, the Minority has repeatedly sought to receive testimony from the Assistant U.S. Attorney that actually worked on the RegPay case. Also for political reasons, the Majority rushed to the floor H.R. 5319, a bill to prohibit websites with sexual content from being accessed by students in schools and libraries which receive Federal e-rate dollars.

Yet, to this day no one has ever testified that children are in danger of online predators in schools or libraries. In fact, testimony has been just the opposite. Children are actually safer when surfing the net at schools or public libraries. So surfing the net alone at home makes children susceptible to child predators, not schools and not libraries. H.R. 5319 is nothing more than an empty political gesture. Mr. Chairman, the parents of this country expect us to protect our children from the threats posed by the 50,000 predators that the FBI says are on the Web searching for our kids right now. Law enforcement has pleaded for our help. Other countries do a much better job of combating online child pornography than here in the United States.

Today we will hear from the financial institutions. I believe it is their responsibility to insure that their firms are not being used as conduits to further child pornography. To date, financial institutions' due diligence has been lacking. Child pornographers, with financial institutions' help have grown their perversion into a multi-billion dollar industry. Depictions of child rape and sexual abuse have been facilitated by credit cards, wire transfers, and other financial transactions. If the financial industry cannot or will not stop providing the financial conduit which created this multi-billion dollar industry, Congress must step in to stop this trade.

If the financial industry faced substantial fines for facilitating child pornography and other unlawful acts over the Internet, I suspect the American people would see a substantial effort to self police themselves. Simply the old adage of see no evil will not fly. Some credit card companies, banks, and other financial institutions have recently stepped up to the plate and have been partnering with the National Center for Missing and Exploited Children to try to cut off the money to commercial child porn sites.

I know Ernie Allen of the National Center is excited about the potential for this new financial coalition. I look forward to hearing from him today about the efforts of some of the financial firms that will be testifying later today. Still I am particularly troubled by the new digital currency. One digital currency company testifying today is Eagle. Digital currency companies are completely unregulated by the Federal government. They are largely based off shore. My fear is that any efforts by Visa, MasterCard, American Express, or PayPal to crack down

on the use of their credit cards to purchase child pornography may be undermined if these digital currency companies are allowed to flourish.

Mr. Chairman, there are important steps we can and should take before adjourning in the next week or so including holding financial institutions responsible for facilitating Internet sales of child pornography. Instead of campaign ads the American public deserves a comprehensive, bipartisan response to this daily threat to our children. With that, Mr. Chairman, I thank you and I yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Stupak. At this time, I recognize the gentleman from New Jersey, Mr. Ferguson, for his opening statement.

MR. FERGUSON. Thank you, Mr. Chairman. I am pleased that you have called this hearing, and I am pleased that we have such a distinguished panel of witnesses, and we certainly shouldn't be complaining that we have the best people in the business, the most expert people, and, frankly, the people with the track record of success in combating this problem. I am delighted that we have this panel with us here this morning, and I thank you, Mr. Chairman, for helping to put it together. Throughout the several months that our committee has explored this problem from numerous different angles, it never ceases to astonish me how horrific this industry is and how it succeeded in rooting itself in our society while avoiding the detection of law enforcement and educators and lawmakers, and, most importantly, of parents.

I would like to thank all of our witnesses for taking time from their other work to join us here today. I have had an opportunity to visit the center and appreciate very much the work that you are doing there and your staff, and I am particularly pleased that our U.S. Attorney from New Jersey is here who has been a leader in combating this problem and sharing his expertise with the committee. This is the second time Mr. Christie has appeared before our committee. The first was at a hearing held in our district in New Jersey at Raritan Valley Community College. Chris Christie, our U.S. Attorney, has been a tremendous asset not only to the State of New Jersey, but also to this particular topic. I can think of no better witness to share with us his experience in tracking financial records to capture and prosecute these people who are going to exploit our children online.

The RegPay investigation that our Chairman just mentioned which was led by Mr. Christie was a landmark child pornography case in my home State that led to the arrest and conviction of numerous individuals for child pornography. This case was the first large scale effort to target the operations of commercial websites offering access to child pornography over the Internet by tracking their financial trail. Also, in

Operation Falcon agents pursued the consumers of child pornography by following the transaction history of those who gained access to the RegPay supported child pornography websites.

Through February of this year information acquired through the RegPay investigation has resulted in 341, 341 Federal, State, and local arrests, and over 700 international arrests. The defendants include teachers, pediatricians, ministers, psychologists, all people who are frequently considered pillars of their community, and who in theory should be dedicating their lives to helping others. Despite how large these numbers may appear, we know this really barely scratches the surface of the problem. However, it is clear that these financial investigations work to capture people involved in these activities. I look forward to hearing from our witnesses today, and how we can continue and strengthen these investigations and hopefully put more people who prey on our children behind bars.

Unfortunately, child pornography sites are not the only area where the reputable credit card logo is confusing and even misleading to the public. Mr. Chairman, I know this is slightly off topic but I am hopeful that next year we will consider looking at other ways that this companies deal with sites where fraud is sometimes also a problem and where music is made available to consumers through sites that don't have required licenses. We spent a lot of time in our full committee talking about the problems of piracy, and we have enacted laws to criminalize the theft of copyrighted and trademark work. But there are more than a few illegitimate websites trafficking in pirated music and other products, and consumers may believe that these sites are legitimate because the transactions are completed with credit cards that all of us have come to trust.

Again, I want to thank our witnesses. I look forward to the opportunity to further introduce Mr. Christie in a moment, but I thank you, Mr. Chairman, for calling this hearing, and I look forward to the testimony.

MR. WHITFIELD. Thank you, Mr. Ferguson. At this time I recognize Ms. DeGette of Colorado.

MS. DEGETTE. Thank you, Mr. Chairman, and I am very grateful as the other Members are that we are holding this in another series of investigatory hearings on child exploitation on the Internet. We have been shocked, I think, all of us, at the growing problem, and I think all of our constituents should be very concerned about how pervasive child pornography on the Internet is becoming. As we now know from previous hearings predators have taken to using the Internet to hurt our children, to buy and sell pictures and videos of rape and torture, and also to exchange the pictures among themselves.

Now in the latter category who were exchanging the images are now becoming engaged in the practice of sharing the collections with people-- are not involved in just sharing them with people who give them new photos, but now what is happening is experts are saying this is partially responsible for the rise in that type of crime because people who used to just get the photographs are now themselves becoming perpetrators. This poses a whole new level of danger to children who travel unwittingly in the spheres of these pedophiles. And, Mr. Chairman, we looked at this issue from a number of different angles and you mentioned some of the different ideas that we have had coming out of these hearings.

One of them that the Chairman mentioned is from Internet service providers whose networks have been hijacked by these despicable criminals, and so I have been working on the legislation that the Chairman mentioned in order to combat this crime. What the legislation does, and it is a bipartisan bill, we have been working with Chairman Whitfield and also with the Chairman of the full committee, Mr. Barton, to mandate that all of these Internet service providers retain IP addresses for the period of a year. This is consistent with 49 attorney generals who have recommended this, as well as the Chairman said the Attorney General of the United States last week.

This might seem like a minor requirement to some people. We are not requiring the retention of the communications themselves, but rather identifying data so that law enforcement officials if they had probable cause to believe that a crime was being committed could go in and get a subpoena and subpoena these addresses. We have heard compelling testimony from more than one witness that one of the single biggest impediments to capturing these terrible perpetrators is the destruction of the identifying data because the law enforcement officials cannot go in and subpoena the location of the perpetrators. The perpetrators close down their accounts and they move location, and so tragically we never find the perpetrators and we never find the children who are their victims.

And so some people have talked to me about privacy considerations. I am concerned about privacy considerations too, especially in light of some of what I believe to be the illegal surveillance of Americans' telephone records by the Administration, but I have got to say we already require telephone companies to keep this information for a 1-year period. We are not requiring content and ISPs across the board do retain this data for some period of time right now. So all we are doing in this legislation is requiring a standard in the industry, and we are requiring very strict probable cause to be shown by law enforcement before the data can be released.

Mr. Chairman, I bring this up because my staff has been working diligently with your staff, and I would hope--we have a bill that is almost complete. I would hope we would be able to introduce this legislation before we left at the end of next week.

MR. WHITFIELD. Well, I hope we can as well and appreciate the great effort you are making.

MS. DEGETTE. Thank you so much, Mr. Chairman. Finally, I am very glad to see the witnesses who are in here today. I think that we can learn greatly about ways to combat this crime from the testimony we will hear. And, finally, Mr. Chairman, I would say that every Internet home page, social networking and chat room site and sites of this nature should have something similar to the virtual global network button that will permit children approached by a predator to immediately report the approach to law enforcement. I think that reporting technology can be very useful for kids. I think they will use it, and I hope we can work with industry and with the ISPs to make this happen. Thank you so much, Mr. Chairman, and I yield back.

MR. WHITFIELD. Thank you, Ms. DeGette. At this time I recognize the gentlelady from Tennessee, Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman, and I also want to thank you for holding the hearing and for you putting your attention and your staff's attention on the issue. I also want to thank our witnesses and welcome them. We look forward to hearing the information that you have for us today. We realize that we need to know what you know. Online child pornography is an ever increasing avenue that child predators are using to exploit our children. It is unfortunate, but it is one that we are going to have to work together to address. Millions of images and videos of these acts are being transmitted daily over the Internet, and it is now a multi-billion dollar industry in the United States, and one that is of tremendous concern to us.

As law enforcement must be diligent to investigate these crimes the financial services industry must insure that it is not providing economic avenues for people or businesses to obtain financial gain from these illegal activities. Child pornography is a horrible and detestable mark of society and people who want to watch, copy, and sell this to others should be punished. The Chairman should be applauded for having this hearing today so that we can insure that the financial services industry is doing all it can to prohibit the financial transactions that support this activity. The committee has held hearings, several hearings now, on the sexual exploitation of our children, and Congress has passed several measures to begin addressing the situation.

As my colleague from Colorado mentioned, there are other pieces of legislation that are yet to come before us. On July 27, '06 the Children

Safety Act was signed into law and implements a nationwide sex offender registry and enhanced criminal penalties for crimes against children. We have also put measures into place to help prevent the human sex trafficking of women and children through the authorization of the Trafficking Protection Act. I do look forward to the testimony today, and to future hearings on other issues such as Mr. Ferguson mentioned in his opening statement on how Congress can assist the financial service industry and law enforcement in making certain that we address online child pornography and other issues of fraud and deception. Again, I thank the Chairman for looking into the delicate issue and welcome you all to our panel.

MR. WHITFIELD. Thank you, Mrs. Blackburn. At this time I recognize the gentleman from Texas, Dr. Burgess.

MR. BURGESS. Thank you, Mr. Chairman, and thank you for this continuation of these very important series of hearings. As you have already pointed out, we have had several, and over these last several months our committee has taken up the important cause of protecting our children from sexual exploitation over the Internet. It is hard to judge your emotions on a subject like this. For myself, they range from shock and disbelief to a strong desire to completely eradicate this problem. I have learned a great deal more than I have ever wanted to know about this subject, Mr. Chairman, but it is crucial for the safety of our children for all of us to know about these evils so that we can help end this abusive and pernicious practice in our society.

While the pedophiles are our biggest enemy, we must also continue to look and combat every ancillary agency associated with this crime. The philosopher journalist H.L. Minkin used to admonish us to follow the money. Well, I am glad today that we are focusing on the efforts of the financial industry. The representatives from reputable credit card companies will provide a valuable insight into what their respective companies are doing. I am also very interested in discussing with Dr. Douglas Jackson and his company, e-gold. I frankly do not understand the need for completely anonymous digital currency, and look forward to hearing from Dr. Jackson about his company's due diligence and role in stopping illegal activities like child pornography.

Today we also have with us Mr. Ernie Allen, the President and CEO of the National Center for Missing and Exploited Children, who will be discussing the creation and the role of the financial coalition against child pornography at the National Center. From my understanding it has been reported that Mr. Allen believes that the financial coalition can eradicate commercial child pornography by 2008. I think I can speak on behalf of the rest of the committee that we would all like to learn more about how he thinks this goal is attainable. I do appreciate the efforts of

my colleague from Colorado and her efforts to get legislation that would enforce the stability of the financial data. Currently it seems that so many of these numbers just evaporate in the ether and we are unable to trace these problems to their source, and I look forward to learning more about her legislation.

And, Mr. Chairman, I too would add my voice to perhaps that is something that this committee could look at getting done before the end of the year. Mr. Chairman, I thank you again for your continued leadership and your dedication to this grave situation. I know it is unpleasant. I know it is difficult, but it is work that we must do. I look forward to working with you and others on the committee as we continue to seek solutions to this most egregious problem. It is my sincere hope that this hearing will be a catalyst for more legislation aimed at curbing this problem.

MR. WHITFIELD. Thank you, Dr. Burgess. At this time I recognize Mr. Barton, the Chairman of the Energy and Commerce Committee, for his opening statement.

CHAIRMAN BARTON. Thank you, Mr. Chairman. Over the last 9 months, the subcommittee has investigated extensively the issues surrounding the sexual exploitation of children over the Internet. Today's hearing is the sixth on this obnoxious subject. We have listened to witnesses involved in all aspects of the fight against Internet child pornography, including Federal and State law enforcement officials, prosecutors, National Center for Missing and Exploited Children, educators, government officials, and Internet service providers.

I think it is clear that this fight cannot be won by law enforcement alone. Internet child pornography is an epidemic in every sense of the term and it will only be wiped out if everyone joins the fight. A high priority will be shutting off the flow of money. Commercial child pornography is big business because as law enforcement officials and others have testified, it makes so much money and the payment mechanisms have become so sophisticated and complex participation of the financial industry in this fight is absolutely essential. If the criminals who operate commercial child pornography cannot be paid, they lose the incentive to create the images of sexual abuse that titillate child predators.

We must have the cooperation of the financial industry in identifying and plugging the payment channels, shutting down the businesses and merchants who profit from the pain and abuse inflicted on innocent children. From the written testimony for today's hearing it appears that the financial industry is making progress towards this goal. I understand that due to the credit policies and monitoring practice of the credit card associations and acquiring banks these institutions have seen relatively

few cases of merchants processing child pornography credit card payments on their system. I commend you for this, but I also hope you continue to be aggressive and creative in implementing solutions that will prevent these businesses from using your payment systems.

For this reason, I am interested in learning more about how you identify merchants who were engaged in child pornography and how those merchants seek to evade your detection. In addition, I would like to know what action you take once you discover that a merchant is engaged in child pornography. For instance, do you terminate this merchant's account immediately? Do you take steps to make sure the merchant's website is shut down immediately? How do you prevent that business from again signing up as a merchant maybe under another name with your institution? Finally, how do you interact with law enforcement with respect to any investigations that are ongoing?

I have posed many of these questions to witnesses for the FBI when they testified, and I am interested in your perspective. In addition to the financial companies appearing before us today, we are joined by Mr. Ernie Allen for the National Center for Missing and Exploited Children. Once again, the National Center has led the fight by helping to establish this financial coalition against child pornography. I want to congratulate Mr. Allen and the National Center for their dedication.

Finally, we are going to be joined by two members of law enforcement, United States Attorney for the District of New Jersey, Chris Christie, and Mr. James Plitt, Director of the Cyber Crimes Center at the United States Immigration and Customs Enforcement. Mr. Christie's and Mr. Plitt's offices conducted their RegPay investigation and prosecution. I look forward to learning from them about the payment systems that are being used by child pornography websites and what challenges these systems pose to their investigations. If there is something that the Congress can do to provide any of these individuals with the tools that they need to investigate these websites, we want to learn about it at this hearing today.

Again, Chairman Whitfield, Ranking Member Stupak, thank each of you for your personal dedication to this subject. With that, I yield back the balance of my time.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Chairman Whitfield, for convening this hearing.

Over the last nine months, this subcommittee has investigated extensively the issues surrounding the sexual exploitation of children over the Internet. Today's hearing is our sixth on this obnoxious subject. We've listened to witnesses involved in all aspects of the fight against Internet child pornography, including federal and state law enforcement



officials, prosecutors, the National Center for Missing and Exploited Children, educators, government officials, and Internet Service Providers. I believe it is clear that this fight cannot be won by law enforcement efforts alone. Internet child pornography is an epidemic, and it will only be wiped out if everyone joins the fight.

A high priority will be shutting off the flow of money. Commercial child pornography is big business because, as law enforcement officials and other witnesses have observed, it makes so much money and the payment mechanisms have become sophisticated and complex, the participation of the financial industry in this fight is essential. If the criminals who operate commercial child pornography sites cannot be paid, they will lose the incentive to create those images of sexual abuse that titillate child predators. We must have the cooperation of the financial industry in identifying and plugging the payment channels and shutting down the businesses and merchants who profit from the pain and abuse inflicted on innocent children.

From the written testimony, it appears that the financial industry has made significant progress toward this goal. I understand that, due to the credit policies and monitoring practices of the credit card associations and acquiring banks, these institutions have seen relatively few cases of merchants processing child pornography credit card payments on their systems. I commend you for this, but I also hope that you continue to be aggressive and creative in implementing solutions that will prevent these businesses from using your payment systems. For this reason, I am interested in learning more about how you identify merchants who are engaged in child pornography and how these merchants seek to evade your detection. In addition, I would like to know what action you take once you discover a merchant is engaged in commercial child pornography. For instance, do you terminate this merchant's account immediately? Do you take steps to make sure that the merchant's website is shut down? How do you prevent that business from again signing up as a merchant with your institution? Finally, how do you interact with law enforcement with respect to these investigations? I posed many of these questions to witnesses for the Federal Bureau of Investigation when they testified at our hearing in May, and I am interested in learning your perspective.

In addition to the financial companies appearing before us today, we are joined by Mr. Ernie Allen of the National Center for Missing and Exploited Children. I understand that, once again, the National Center has led the fight by helping to establish the Financial Coalition Against Child Pornography. I would like to congratulate Mr. Allen and the National Center for their dedication, and I look forward to learning more about the Financial Coalition's work.

Finally, we are joined by two members of law enforcement, United States Attorney for the District of New Jersey Chris Christie and Mr. James Plitt, Director of the Cyber Crimes Center at United States Immigration and Customs Enforcement. Mr. Christie's and Mr. Plitt's offices conducted the Reg Pay investigation and prosecution. I look forward to learning from them about the payment systems that are being used by commercial child pornography websites and what challenges these systems pose to their investigations. If there is something that Congress can do to provide you with the tools you need to investigate these websites, I would be interested in learning this as well.

Again, I thank Chairman Whitfield for convening this hearing and I yield back the balance of my time.

MR. WHITFIELD. At this time I recognize the Vice-Chairman of the Energy and Commerce Committee, Mr. Pickering of Mississippi.

MR. PICKERING. Mr. Chairman, I thank you for all your work in this area to protect our children and our families. I look forward to hearing the testimony today and working with the committee. I do think that enhanced enforcement, the tools, the resources, the commitment to do

whatever it takes to address this issue. I am also looking at legislation that would look at means to address the financing or the purchasing and acquisition of child pornography but other age-restricted products like alcohol and tobacco so that we can have a comprehensive approach, common sense approach that if we can stop the purchase and take away the financial incentives then hopefully we can make some progress to prevent before we have to enforce.

I look forward to working with the Chairman on that legislation and other concerned groups so that we can advance and work in the next Congress to address these very critical issues. Chairman Whitfield has done a tremendous job in bringing everyone's attention and educating and informing. Now is our time and our responsibility to act. Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Pickering. And at this time, I want to welcome the first panel, and for the purpose of introducing the first witness on the first panel, I recognize the gentleman from New Jersey, Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman. I am pleased to recognize and introduce the Honorable Christopher J. Christie. He is the United States Attorney for the District of New Jersey, my home State. I have known Mr. Christie for a number of years and in his 5 plus years as the U.S. Attorney in New Jersey, he has built an extraordinary reputation of integrity and effectiveness in a number of different areas. He has been successful in one area in particular. I will mention several, but in the area of public corruption he has 97 public corruption guilty pleas or convictions. That is 97 and 0.

These are folks from both sides of the aisle. He has been a leader in combating human trafficking. He has been a leader in combating terrorism and advancing homeland security in New Jersey. He has had done some extraordinary work in corporate and non-profit governance. I would venture to say that his record as U.S. Attorney is second to none across this country, and we are very, very pleased and fortunate that he has been able to take some time from his responsibilities in New Jersey.

In addition to the work that he has done on RegPay and some of the things I mentioned in my opening statement, we are very, very pleased he is able to be here to share with us some of his experience, so I am delighted to welcome Chris Christie, the U.S. Attorney from New Jersey.

MR. WHITFIELD. And in addition to Chris Christie, our witnesses on the first panel will be Mr. Ernie Allen, who is President and Chief Executive Officer of the National Center for Missing and Exploited Children, who is doing a tremendous job in this area and we appreciate your efforts. Also, Mr. James Plitt, who is the Director of the Cyber Crimes Center, Office of Investigations, U.S. Immigration and Customs

Enforcement at the U.S. Department of Homeland Security, and we welcome you Mr. Plitt.

As you all know, this is an oversight investigations hearing. It is our custom to take testimony under oath. Do any of you have any objection to testifying under oath this morning? If you would stand, I would like to swear you in.

[Witnesses sworn]

MR. WHITFIELD. All of you are now under oath, and, Mr. Christie, we will recognize you for a 5-minute opening statement.

**TESTIMONY OF HONORABLE CHRISTOPHER J. CHRISTIE,  
UNITED STATES ATTORNEY, DISTRICT OF NEW  
JERSEY, U.S. DEPARTMENT OF JUSTICE; ERNIE ALLEN,  
PRESIDENT AND CHIEF EXECUTIVE OFFICER,  
NATIONAL CENTER FOR MISSING AND EXPLOITED  
CHILDREN; AND JAMES PLITT, DIRECTOR, CYBER  
CRIMES CENTER, OFFICE OF INVESTIGATIONS, U.S.  
IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S.  
DEPARTMENT OF HOMELAND SECURITY**

MR. CHRISTIE. Thank you, Mr. Chairman, and thank you, members of the committee, for asking me to come here today and talk about a topic that is obviously very important to our office and to the country as a whole. I want to thank Congressman Ferguson for his very kind introduction as well. I would like to talk, Mr. Chairman, about the RegPay case that has been referenced a number of times in your comments and the comments of the other members of the committee. The first important thing to know about the RegPay case is something to understand about Federal law enforcement, and that is that one small group of people can make an enormous difference if they want to be creative and attack a problem on a personal level.

And in our office one Assistant United States Attorney came to me with an idea of wanting to combat child pornography in a different way. And we sat and talked a great deal about it and got buy-in from our other Federal law enforcement partners to undergo an operation which became the RegPay case. The idea behind that was previous to this law enforcement's approach had generally been to follow the purchaser of child pornography and try to trace that back. Most of the arrests that were done were of the people who were buying child pornography over the Internet, and you never got much beyond that.

What we decided to do in New Jersey was to take the approach of following the money as someone mentioned before in their opening remarks. We decided that what we wanted to do was try to get at the

people who were putting these websites up, exploiting the children in the first instance, and also get the money launderers and the middle men who were processing these transactions for them and allowing them to profit. We never believed when we started where this case would take us. It took us from United States in New Jersey, purchasers there, to money launderers and middle men in the State of Florida, to child pornographers in Belarus, and financial institutions in Latvia.

And through the great resources of immigration and customs enforcement, the IRS, and our office, we were able to trace that money. And what it did was our first step was in going after the money launderers, the middle men who were in the United States and Florida. Once we were able to get enough evidence against them to execute search warrants on both their computers and other documents they had to firm up our case against them, we encouraged them and were able to convince them to cooperate with us in our investigation.

Once they began to cooperate, they were able then to able to contact their source people in Belarus, and from there using them and using them as a lure to bring them, the people from Belarus, to a country where we could have the foreign government participate in the arrest and then be able to extradite them to the United States. These few people in Belarus were gathering child pornographic images that were incredibly disturbing, incredibly exploitive of children. And we were able to lure these folks who were making about \$2 million a month on average just from the few websites that they ran. We were able to lure them to France under the guise that we the Florida company was willing to up the ante and process even more of the illicit profits for them and longer.

We got them there. We were able to engage in conversations with them there which confirmed their very, very deep role in this plot. We were able to tape those conversations. Arrests were executed, eventually extradited to the United States, and all of these people in the RegPay case have now pled guilty and they are doing sentences ranging anywhere from 17 years to 25 years in Federal prison for the crimes that they committed. We believe what we did in the RegPay case was to lay out a template for how these cases should be done. And we are seeing that incorporated into the Department's Project Safe Childhood initiative as well now and being sent around the country to work with organizations like the National Center, to work with local law enforcement which we need to have as a partner. It is a three-legged stool. Federal law enforcement must have the help from local law enforcement and from these non-governmental organizations to be able to make this work.

The RegPay case is an enormous triumph for law enforcement in protecting children, and it should be used now, and I think is being used now, as a model around the rest of the country on how to investigate

these cases. And so I am enormously proud of the work that our office did, our assistants and our investigators, and I think they have laid this out now for other people to use, and I know it is being used today by my colleagues around the country as a real example of how to do this kind of work and we are enormously proud of what happened here, Mr. Chairman.

[The prepared statement of Hon. Christopher J. Christie follows:]

PREPARED STATEMENT OF THE HON. CHRISTOPHER J. CHRISTIE, UNITED STATES  
ATTORNEY, DISTRICT OF NEW JERSEY, U.S. DEPARTMENT OF JUSTICE

Chairman Whitfield, Ranking Member Stupak, and distinguished members of the Subcommittee, thank you for inviting me to testify before you today about my office's prosecutions of cases involving the sexual exploitation of children on the Internet, including the RegPay case, in which we prosecuted both producers and consumers of child pornography.

#### **Introduction**

As this Subcommittee is already no doubt aware, the advent of the Internet has led to a vast proliferation in the availability and prevalence of child pornography in today's society. The possession and distribution of child pornography were once relatively rare crimes relegated to those who would frequent certain underground adult bookstores or attempt to order obscure magazines from overseas. The Internet has dramatically changed that by making child pornography easy to produce and distribute, while also making it readily available to those inclined to seek out this material from their own home. Sadly, thousands of individuals who are sexually attracted to children now have ready access to images and videos depicting the sexual exploitation and molestation of children. Moreover, unscrupulous and opportunistic individuals both here and especially abroad have seized the opportunity to market access to child pornography in an industry that provides huge profits and relatively low overhead costs. It is probably accurate to say that the number of individuals in this country who have intentionally obtained access to or traded images of child pornography within the last six-month period outstrips the number for a similar six-month period from 15 years ago by at least a hundredfold. In addition, the Internet has also become an avenue for child predators to seek out and communicate with children in the seeming anonymity of chat rooms.

Needless to say, this sea change has created a tremendous challenge for law enforcement -- one that requires law enforcement to adapt quickly to a rapidly changing landscape and to search for innovative ways to identify and apprehend offenders. It has also put a premium on law

enforcement officers with technological and computer expertise.

Law enforcement efforts to interdict Internet-based child exploitation crimes are largely dictated by the nature of the offense, which can be loosely grouped into two categories: child pornography offenses and child exploitation cases. The former type of investigation is more heavily dependent on technological expertise and forensic investigation, while the latter is typically dependent on the capacity of an individual agent to convincingly portray himself or herself as a minor who is susceptible to advances by on-line predators.

To understand child pornography offenses and the efforts of law enforcement to effectively investigate them, it is necessary to understand the nature of child pornography on the Internet. Much of the proliferation of child pornography can be traced to the existence of numerous commercial websites that offer access to child pornography for a monthly fee. During the past ten years, hundreds of websites, many based in Eastern Europe, have appeared on the Internet. These sites typically require a subscriber to submit various information including billing information, whether it be via credit card or some other on-line payment service such as E-Gold. Law enforcement efforts to interdict these websites and to apprehend both those who operate them and those who subscribe to these sites has proven a formidable task, but there have been notable successes. Foremost among these successes has been the RegPay investigation which represented the collaboration of a number of federal agencies, including ICE, IRS and the Postal Inspection Service in conjunction with the United States Attorney's Office for the District of New Jersey and the Child Exploitation and Obscenity Section in the Department's Criminal Division (CEOS). It is also illustrative of how the federal government can successfully target the commercial child pornography industry at both the level of the producer and the consumer.

#### **The RegPay Case**

The RegPay investigation, which began in early 2003, represented the first large-scale effort to target the operators of commercial websites offering access to child pornography over the Internet and to track the financial trail created by those who profit from this industry. In the early part of that year, federal agents made undercover purchases of monthly subscriptions to numerous child pornography websites in an effort to track down the producers of the material and the operators of the sites. The investigation revealed that a company based in Belarus, which called itself RegPay, operated several commercial child pornography websites and processed credit card fees for more than 50 other similar sites. The investigation also determined that credit card payments for access to these sites were being processed through a company based in Ft. Lauderdale, Florida known as Connections, USA. Agents also executed search warrants on computer servers based in Texas and Virginia that RegPay had leased, and recovered extensive databases documenting credit card transactions involving approximately 90,000 customers worldwide. Armed with this information the investigation pursued two paths, aimed at, on the one hand, the operators of RegPay and those who processed their transactions, and, on the other hand, the consumers who purchased access to the site.

To pursue the operators of RegPay, agents first executed a search warrant at Connections,

USA in Ft. Lauderdale. Upon executing the search warrant, agents learned of an ongoing financial dispute between Connections, USA and the operators of RegPay relating to an outstanding debt of more than one million dollars supposedly owed to RegPay. Agents were able to assume the role of Connections, USA to broker a meeting in Paris between the operators of RegPay and Connections, USA, ostensibly to resolve the ongoing dispute and to set the groundwork for future financial cooperation between the companies. This ruse led to the arrest of two Belarussians in Paris while a third individual was apprehended while vacationing in Spain at the same time. All three were extradited to New Jersey to face charges relating to the production and distribution of child pornography. All three pled guilty on the eve of trial in February of 2005 before the Honorable Dennis M. Cavanaugh of the United States District Court of New Jersey. The two principals of RegPay, Yavor Zalatarou and Aliaksandr Boika, are expected to be sentenced later this month. They face presumptive sentences in the range of 25 to 30 years. In total, 9 individuals pled guilty in the District of New Jersey for their involvement in operating or supporting RegPay's business operations, including three individuals from Connections, USA as well as three California-based individuals involved in the laundering of RegPay's proceeds. One of these latter individuals, Yaroslav Grebenshikov, admitted that in late June 2003, he assisted individuals associated with Regpay in the formation of LB Systems - a company created to assist Regpay and others in Belarus to process credit card sales for previously approved transactions involving child pornography - as well as the opening of a bank account, both of which he used to transfer more than \$200,000 in funds associated with RegPay to banks in Latvia.

Simultaneously, in what was dubbed Operation Falcon, agents pursued the consumers of child pornography by following the transaction history of those who had gained access to the RegPay-supported child pornography websites. By comparing the transaction data obtained via the search warrants conducted on the servers in Texas and Virginia with credit card records, agents were able to seek search warrants for numerous individuals throughout the United States. Leads were also distributed worldwide to pursue those who knowingly received and possessed child pornography. Through February of 2006, the RegPay investigation had resulted in 341 federal, state and local arrests in the United States and approximately 703 additional international arrests. In the District of New Jersey alone, more than 50 individuals were charged federally with possession of child pornography. The New Jersey defendants included teachers, a pediatrician, a psychologist, a retired minister and, perhaps least surprisingly, several individuals who had been convicted of sex offenses against minors, including a former school principal.

#### **Recidivist Offenders**

This latter category illustrates the importance of pursuing the consumers of child pornography because, among other reasons, the link between those who seek out child pornography and those who molest children is substantial and disturbing. Of the approximately 52 New Jersey targets charged federally in New Jersey, 5 had prior convictions for sexual offenses against minors. In addition, 3 other defendants, when confronted by ICE agents conducting searches on their computers, admitted to molesting a total of at least 14 children, while two defendants, including one of the convicted sex offenders, admitted to attempting to meet minors in on-line chat rooms. What cannot be known is how many others of those who were arrested had

molested in the past but chose not to reveal this to authorities. While it is uncertain what percentage of those who gain access to child pornography act out upon their impulses, it is clear that a significant percentage do and common sense dictates that the exposure to child pornography encourages this behavior. For example, a study completed in 2000 by the Director of the Sex Offender Treatment Program at the Butner Federal Correctional Complex in North Carolina revealed that of 54 inmates convicted of child pornography offenses, 79.6% of them admitted that they had also molested significant numbers of children.

#### **Harm to Exploited Children**

Furthermore, the proliferation of child pornography websites and the great profits reaped by their operators fuels a market for the production of new and often hard-core child pornography. In short, the market in child pornography directly leads to the exploitation and molestation of children from all over the globe, often for the purpose of commercial gain. Many of the victims are from Eastern Europe where a substantial percentage of child pornography is produced. Images and videos of American children are encountered with great frequency, however, because once a photograph of child pornography makes its way on to the Internet - something that can be accomplished with ease in the era of digital photography - control of that image is essentially lost, and commercial websites may include such images in the collections they offer on their sites. Sadly, the victimization of children forced to become the subjects of child pornography thus continues as the image travels throughout the Internet. As Attorney General Gonzales noted recently, "[child pornography] is not a victimless crime. Most images today of child pornography depict actual sexual abuse of children. Each image literally documents a crime scene."

#### **The Evolving Landscape and Law Enforcement's Challenge**

As with most sophisticated criminal enterprises, the purveyors of child pornography adapt to law enforcement techniques, thus forcing investigators to adjust to an ever-changing landscape. The commercial child pornography industry has evolved even since the RegPay investigation. For instance, child pornography websites are not as easily located on the Internet by the uninitiated as was the case three to four years ago. While this may reduce the number of individuals subscribing to these sites, it also makes them harder for law enforcement to locate and identify. Moreover, the operators of these sites are increasingly sophisticated in hiding their own identities and whereabouts. They accomplish this both technologically - by making their operations more difficult to trace through the use of such software as anonymizers - and by insulating themselves through the use of sham Internet-based companies and other third parties through which they funnel their profits from the child pornography websites. Moreover, they lease server space typically through the use of stolen identities, and the companies that lease the space to them frequently do not realize the true content of the website they are helping to host. Perhaps the greatest challenge to bringing these individuals to justice, however, stems from the concentration of such operations in Eastern Europe, typically in the break-away Soviet republics such as Belarus. Most of these countries do not have extradition policies with the United States, and the knowledge of the fate of the RegPay defendants makes the likelihood that operators of similar sites will venture outside the relative safety provided by the borders of their home country remote at best.



Widespread corruption amongst Government officials in some of these countries significantly reduces the chances that they will face meaningful prosecution in their homeland.

These obstacles mean that curbing demand for child pornography will be increasingly important in combating the proliferation of this material. Techniques including electronic surveillance and the execution of search warrants on servers both domestically and abroad provide a deterrence effect for those who might seek child pornography through online commercial websites. Law enforcement needs to send a clear message that individuals who subscribe to these websites and contribute to the molestation of children across the globe run a substantial risk of facing significant jail time any time they hit the "JOIN NOW" button for one of these sites. As I speak here today, even though child pornography websites are harder to locate than before, there are still thousands of Americans who attempt to subscribe to child pornography websites every month. Law enforcement can and will play a significant role in bringing such individuals to justice.

#### **Alternative Distribution Methods**

While I have spoken so far primarily about the role of commercial websites in the proliferation of child pornography, it is important to realize that a great deal of child pornography gets distributed on the Internet through individuals who trade such material with one another. Additionally, peer-to-peer software such as Kazaa and Limewire may be abused by those with a mutual interest in child pornography to share their respective collections with one another if they belong to the same network of computers. Child pornography may also be distributed through attachments to e-mail. Individuals with an interest in child pornography may frequent certain chat rooms from which they will exchange collections. In addition, certain individuals may establish on their home computer what is known as an F-Serve on which they establish a collection of child pornography that can only be accessed by those who upload images of child pornography to the F-Serve first - thereby preventing law enforcement from gaining access while expanding the F-Serve operator's own collection.

All of these methods for distributing child pornography cause many of the same harms as posed by commercial child pornography websites, namely, the continued victimization of the children depicted and the encouragement of those with pedophilic impulses to act upon them. Law enforcement can identify many of the individuals involved in these forms of distribution through a variety of techniques. For instance, certain programs can be run which search computers that are connected through the same network for a particular image as defined by its hash value. This enables law enforcement to identify individuals who have particular images of child pornography on their computers and may establish sufficient probable cause for search warrants. In addition, forensic examination of an individual's computer that has been seized may reveal e-mail communications with other individuals who have sent and received child pornography from the seized computer. In this regard, traditional cooperation from a defendant who has distributed child pornography through these means may lead to the identification and arrest of numerous others.

### **Interstate Traveler Cases**

In addition to investigations involving child pornography, the Federal Bureau of Investigation plays a vital role in preventing and even interdicting child exploitation crimes so long as there is some interstate nexus to provide federal jurisdiction. The best known example of this type of investigation is the so-called enticement or "traveler case," which has been recently well documented on a series of "Dateline NBC" episodes. Across the country, too many of our children have been lured by child abusers through contacts in chat rooms that are allegedly closed to adults. Some of these interstate travelers also take pictures of the minors they molest and sometimes abduct, and then post the child pornography online. This type of investigation requires an undercover agent to enter an Internet chat room where older men are likely to be interacting with minors. The undercover agent will engage in a series of chats to determine if the other individual is an adult seeking sexual contact with the undercover whom he believes to be a young teenager. As the chats progress, the older male may decide to travel to the location of the minor in the hopes of renting a nearby motel room or making similar arrangements. If the older male travels across state lines to meet the minor, the case may be taken federally. While many "traveler cases" may be prosecuted at the state level, federal traveler cases are not uncommon. For instance, the District of New Jersey is currently prosecuting a case where a doctor from a prominent Philadelphia hospital traveled to Hackensack, New Jersey expecting to meet a 14-year old girl with whom he intended to have sexual relations. Such "traveler cases" often involve actual minors whom the traveler intends to sexually abuse. For example, the District of New Jersey recently secured a conviction of a Florida man who traveled to New Jersey to have sex with a 13-year old girl. ICE agents, who did not initially know the identity of the intended victim, trailed the defendant and observed him following a school bus in an effort to find the girl whom he had met over the Internet. The agents were able to interdict this crime before the defendant, who was in possession of a stun gun and alcohol, contacted the victim. It is likely that such crimes, however, are greatly under reported by the young and confused victims.

### **Sex Tourism Cases**

Another, albeit less common type of child exploitation case that may involve the Internet arises out of sex tourism investigations wherein the defendants are individuals who travel overseas to have sex with minors, or who organize such trips. These trips frequently involve travel to southeast Asia. Sex tour operators catering to pedophiles tend to be discreet and are difficult to infiltrate because they are usually extremely wary of law enforcement. If successful, however, these cases may not only lead to the apprehension of the tour operator, but his prior clients as well. Because of the international nexus of these violations, the Bureau of Immigration and Customs Enforcement (ICE) often acts as the primary federal law enforcement agency responsible for conducting such investigations. ICE has conducted many successful child sex tourism investigations and works closely with CEOS, the U.S. Attorney's Offices, as well as federal, state and local law enforcement agencies.

The District of New Jersey is currently prosecuting one such case where the defendant operated a website advertising sex tourism. The website did not specifically advertise that its

tours were catered toward minors, but it included pictures of girls in various states of undress, some of whom clearly appeared to be underage. The investigation involved undercover Internet chats followed by meets wherein undercover agents posed as customers seeking to have sex with underage girls upon arrival in the Philippines. The defendant initially indicated that he would not talk about minors until the group arrived in the Philippines, but he gradually opened up to the point where he admitted to having sex with minors himself.

#### **Project Safe Childhood**

All of the investigations that I have described so far will be bolstered by the Department of Justice's recently launched Project Safe Childhood initiative designed to coordinate the efforts of federal agencies and U.S. Attorneys' Offices with state and local law enforcement. This initiative is designed to help coordinate national child pornography investigations, train additional federal, state and local law enforcement in pursuing computer-based investigations and raise community awareness of the dangers of the Internet for children. The initiative is also designed to increase federal involvement in many of these investigations, especially where state laws provide little deterrence for offenders. This latter point is clearly evident in New Jersey where possession of child pornography regularly results in sentences of 2 to 3 years if prosecuted federally but carries with it a presumption of a probationary sentence under state law.

I am proud that the District of New Jersey has been a leader in pursuing child exploitation offenses on a national level, as evidenced by the RegPay case, which represents one of the most successful child pornography investigations in the nation's history. Most importantly, Project Safe Childhood will ensure that every state and every district has properly trained law enforcement officials who can vigorously pursue predators and similar offenders, when supplied with appropriate leads, and that these investigations will realize even greater success in the future.

I should also note that the District of New Jersey's experience in pursuing RegPay and other similar investigations demonstrates that the number of child pornography and other child exploitation offenders is quite simply staggering, and that it behooves law enforcement offices - whether they be the prosecuting authority or the investigative agency - to devote greater resources and personnel to these investigations. The RegPay investigation demonstrates that a few well-trained and dedicated law enforcement officials can make a major impact and provide prosecutors and agents in their own and other districts with large numbers of dangerous offenders to pursue and bring to justice. Unfortunately, sometimes our own American youth are the victims of traffickers in this country who lure youth from their communities and sell them for prostitution in other jurisdictions, offering them for sex at truck stops, conventions, and on the streets of our cities.

#### **Human Trafficking**

I would be remiss if I did not mention that the impact of federal law enforcement's efforts to protect children is not limited to investigations focused on the Internet. One type of crime that frequently entails the exploitation of minors are those involving human trafficking, whether they

involve forced labor or sex trafficking. Many of the victims of this type of deplorable crime are minors, and they are often sexually exploited on a commercial basis. Human trafficking is a crime that has been with us for many years, but continued largely unnoticed until the passage of the Trafficking Victims Protection Act of 2000, authored by a strong, committed group of legislators including Representative Christopher Smith, from my home state of New Jersey. That legislation recognized that many individuals, typically young female immigrants, were being smuggled into the United States and forced to work in demeaning conditions or in prostitution. Since the passage of that legislation, numerous trafficking cases have been brought throughout the United States, and the District of New Jersey has once again been one of the leaders in pursuing these types of cases.

In 2002, for example, this Office brought the case of *United States. v. Jimenez-Calderon* which led to the convictions of two women for their role in forcing several juvenile Mexican girls to work as prostitutes in Plainfield, New Jersey. The defendants received sentences of approximately 17½ years each. In 2005, this office indicted the case of *United States. v. Luisa Medrano, et al.*, which involved the smuggling into the United States of young Honduran females, some as young as fourteen, after they had been promised legitimate waitressing jobs to lure them into the country. Upon arrival in Union City, New Jersey, these girls were forced to work six or seven days per week at bars catering to male immigrants where they were pressured to perform sexually provocative dances for the customers and ply them with alcohol. The victims were also required to live at specific residences and had their movement greatly restricted until their smuggling debts were paid off in full. Many of these juveniles were sexually exploited during the smuggling process that brought them to New Jersey.

Even more recently, the District of New Jersey has brought various charges against a number of defendants for their involvement in prostitution activities in Hudson County and elsewhere. These defendants are primarily members of the Notario family from San Miguel Tenancingo, the trafficking capital of Mexico. The investigation has identified numerous trafficking victims who were put to work as prostitutes in various brothels along the East Coast after having been smuggled in from Mexico. Among these identified victims are at least three juveniles. Thus, the pursuit of human trafficking cases often represent yet another means by which law enforcement identifies and dramatically assists sexually exploited minors.

### **Conclusion**

In conclusion, the dangers of the Internet in the proliferation of child exploitation crimes cannot be underestimated. The Attorney General has recognized that “we are in the midst of an epidemic in the production and trafficking of movies and images depicting the sexual abuse of children,” and the need for law enforcement to respond rapidly and forcefully cannot be more clear. With proper coordination and the cooperation of federal, state and local authorities, the Internet can be made far safer for the children of this country. Law enforcement must create an environment in which sexual predators fear the Internet as a dangerous place that may likely land them in prison for a significant period of time. The RegPay investigation - especially with the advent of Project Safe Childhood - provides a model for law enforcement agencies throughout the country to pursue child exploitation cases with the knowledge that the offenders who are identified

will be vigorously investigated and prosecuted.

Mr. Chairman, I again thank you and the Subcommittee for the opportunity to speak to you today, and I would be pleased to answer any questions the Subcommittee might have.

MR. WHITFIELD. Thank you, Mr. Christie. At this time, I recognize Mr. Allen for a 5-minute opening statement.

MR. ALLEN. Thank you, Mr. Chairman, Congressman Stupak, members of the committee. First, thank you for your extraordinary leadership and impact on this problem. I have submitted written testimony covering a wide range of issues. However, what I would like

to do in my oral testimony very briefly is to focus on five questions that this committee asked the center to address. The first was raised by Chairman Barton who said to us why can't we in this country do what the British are doing in terms of blocking sites and shutting them down. I think most of you know, and I have expressed to members of this committee that our first priority has always been investigation and prosecution, and identifying who the child victim is, so there is a balance in how we do that.

But based on that idea we met with the leading ISPs and the U.S. Internet Service Provider Association, and we have found that they are enthusiastic about such a mechanism. We subsequently met with our partners in Federal law enforcement and have developed a process that we are now working to implement. The first step is that our analyst at the National Center will identify the illegal sites. Secondly, we will provide these reports to Federal law enforcement, the Internet Crimes Against Children Task Forces. Thirdly, we will add the URLs of these sites to a list and then provide that list to the validated ISPs who are registered with our Cyber TipLine.

Let me emphasize that in the testimony we work primarily with the large ISPs and inadvertently I omitted Yahoo, who is very supportive and very involved in this process. But ultimately all reporting ISPs, the 255 ISPs for reporting content, will receive this list and these notifications. We will advise them of the illegal content in a specific URL and then ask them to enforce their terms of service agreement. This is a violation of those agreements. Thus, they will take down the site, block its future access over their systems using filters, so this is an attempt to give law enforcement first crack at all of the content but simultaneously develop a system that will identify the illegal sites, shut them down, and then block their future access.

So I report this to the committee. This was something the committee was specifically interested in. Secondly, you have asked about new technology, how can we develop technology solutions for this problem. Well, since the last hearing we have met with Internet industry leaders, AOL, Microsoft, Yahoo, Google, Earthlink, and United OnLine. They have committed their best and brightest, and we have created a kind of technology coalition to try to develop new technology to identify this illegal content and interdict it. That process has been formed and is underway, and I will keep you apprised of its progress.

Thirdly, as mentioned in the opening remarks about the poor reporting. I know Congresswoman DeGette, you have been very concerned about that. In our most research, we found that just 5 percent of children who are targeted by online sexual exploitation report it to law enforcement, to AOL, to us at the National Center, and just 12 percent

tell their parents. So overwhelmingly this is a problem that is underreported. As you know, Congress mandated the creation of our Cyber TipLine, and last week we handled our 417,000<sup>th</sup> report. If only 10 percent of the American public is reporting, it is terrifying to think what the volume really could be, and we are very supportive and eager to work with industry to develop new mechanisms including permanent, prominent Cyber TipLine icons and links so that these things can become a virtual panic button for children and can get us far greater reporting volume.

Fourthly, you asked us about modeling sites. We have handled reports on that. In our judgment, many of these sites which hide under the “guise” of the First Amendment are in effect masking other kinds of illegal behavior. We look forward to working with you and your staff on this problem. And then finally you asked about our financial coalition, and let me give you a quick update. We just launched this coalition 6 months ago. We talked about it at your last hearing. Dr. Burgess mentioned our ambitious goal of eradicating commercial child pornography by 2008. Today I am pleased to report that 23 major companies, including leaders of the credit card industry, major banks, Internet service providers, third party payment companies, are all engaged in this process.

Those companies represent 87 percent of the U.S. payments industry measured in dollars running through the system. Our mission as has been discussed is to follow the money, stop the payments, shut down the accounts, and put an end to this multi-billion dollar enterprise. Where we are at this point is we have just completed a pilot phase. We have developed technology and an information sharing methodology which has now been tested and debugged. And we have just launched an effort in which all of these companies will be participating in this process.

While it is too early to provide real conclusions, and law enforcement has urged us not to reveal the specific techniques and methods that we are using in our judgment there is already an encouraging trend. Because of the unprecedented efforts of law enforcement at all levels and others, we believe that these enterprises are already being disrupted. For example, we are seeing that the credit card logos we are finding on these sites in most cases do not lead you to an actual account, and what we are finding is that they are being used for one of two purposes, either identity theft, and if you attempt to purchase access to a child pornography site using a credit card and you don't get your product to whom are you going to report it.

Secondly, they are being used for these sites then to redirect people to other payment methods, and these include a whole array. We don't have a lot of detail yet, but I can assure you working with law

enforcement we are pursuing them and will pursue them as they emerge. The challenges that I present to the committee are really two fold. One, we are very pleased that 87 percent of the U.S. payments industry is involved in this effort. It needs to be 100 percent, and we need your help and support to bring the rest of the financial institutions in this country into the process.

Then, secondly, as you heard from Mr. Christie and you heard from others, this is not just a domestic problem, it is a global problem. We have met with the European Banking Federation. We are meeting with Asian bankers and Central American bankers and Canadian bankers. The goal is to create a real international process. And in closing, Mr. Chairman, what I would like to do is tell you about one company, an international company that is a part of this coalition, Standard Charter Bank, in Singapore, which is helping us mobilize Asian bankers around this effort. They are so motivated that they went to their employees and they raised \$60,000 in employee contributions to create a public awareness campaign.

They have created a website called Light a Million Candles. They are trying to get people around the world to sign on to this process, and they have had responses so far from 130 countries. So in closing what I would like to do is ask that this PSA that the Standard Charter Bank developed be shown to the committee. It is now being shown in Asia, the Middle East, Africa, and expanding world wide. Thank you, Mr. Chairman.

[Video]

[The prepared statement of Ernie Allen follows:]

PREPARED STATEMENT OF ERNIE ALLEN, PRESIDENT AND CHIEF EXECUTIVE OFFICER,  
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Mr. Chairman and distinguished members of the Committee, I welcome this opportunity to appear before you to discuss the commercial distribution of child pornography on the Internet. Chairman Whitfield, I cannot thank you enough for the attention that you, Chairman Barton, Congressman Stupak and your colleagues on the Committee have brought to the problem of child sexual exploitation this year.

The National Center for Missing & Exploited Children ("NCMEC") joins you in your concern for the safety of the most vulnerable members of our society and is grateful for your continued focus on this under-recognized problem.

Let me first provide you with some background information about the National Center for Missing & Exploited Children (NCMEC). NCMEC is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice as the national resource center and clearinghouse on missing and exploited children. NCMEC is a true public-private partnership, funded in part by Congress and in part by the private sector. Our federal funding supports specific operational functions mandated by Congress, including a national 24-hour toll-free hotline; a distribution system for missing-child photos; a system of case management and technical assistance



to law enforcement and families; training programs for federal, state and local law enforcement; and our programs designed to help stop the sexual exploitation of children.

These programs include the CyberTipline, the “9-1-1 for the Internet,” which serves as the national clearinghouse for investigative leads and tips regarding crimes against children on the Internet. The Internet has become a primary tool to victimize children today, due to its widespread use and the relative anonymity that it offers child predators. Our CyberTipline is operated in partnership with the Federal Bureau of Investigation (“FBI”), the Department of Homeland Security’s Bureau of Immigration and Customs Enforcement (“ICE”), the U.S. Postal Inspection Service, the U.S. Secret Service, the U.S. Department of Justice’s Child Exploitation and Obscenity Section and the Internet Crimes Against Children Task Forces, as well as state and local law enforcement. Leads are received in seven categories of crimes:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- child-sex tourism;
- child sexual molestation (not in the family);
- unsolicited obscene material sent to a child; and
- misleading domain names.

These leads are reviewed by NCMEC analysts, who visit the reported sites, examine and evaluate the content, use search tools to try to identify perpetrators, and provide all lead information to the appropriate law enforcement agency. The FBI, ICE and Postal Inspection Service have “real time” access to the leads, and all three agencies assign agents and analysts to work directly out of NCMEC and review the reports. The results: in the 8 years since the CyberTipline began operation, NCMEC has received and processed more than 417,000 leads, resulting in hundreds of arrests and successful prosecutions.

The vast majority of these reports involve images of sexually exploited children. Child pornography has become a global crisis. A recent report by McKinsey Worldwide estimated that today commercial child pornography is a multi-billion-dollar industry worldwide, fueled by the Internet. Its victims are becoming younger. According to NCMEC data, 19% of identified offenders had images of children younger than 3 years old; 39% had images of children younger than 6 years old; and 83% had images of children younger than 12 years old. Children have become a commodity in this despicable crime.

Who is behind this trade in our children? There are documented cases in which the enterprise was found to be operated by an organized crime network. One such case was that of the Regpay Company, a major Internet processor of subscriptions for third-party commercial child pornography websites. The site was managed in Belarus, the credit card payments were processed by a company in Florida, the money was deposited in a bank in Latvia, and the majority of the almost 300,000 credit card transactions on the sites were from Americans.

Another recent case highlights the connection between child pornography and the financial system. In this case, investigators identified 70,000 individual customers paying \$29.95 per month and using their credit cards to access graphic images of small children being sexually assaulted.

This is not acceptable. So we created the Financial Coalition Against Child Pornography, made up of the world’s most prominent financial institutions and Internet industry leaders who have joined with NCMEC and its sister organization, the International Centre for Missing & Exploited Children (“ICMEC”) in the fight against Internet child pornography. There are now 23 members, which include MasterCard, Visa, American Express, Bank of America, Citibank, PayPal, Microsoft, America Online,

Yahoo and many others. We are bringing new financial institutions into this Coalition every day. Our newest member is HSBC North America, and the American Bankers Association has recently agreed to support the Coalition's efforts. These are significant additions to our team.

The members of the Coalition represent 87 percent of the U.S. payments industry, measured in dollars running through the system.<sup>1</sup> This offers great potential to eradicate the commercial child pornography industry. We would have a greater chance of success if we had 100 percent participation by industry players around the world. ICMEC representatives have met with the heads of the European Banking Association as well as with officials from Central American banks. We are also actively recruiting the Asian banks as well.

Our goal: to eradicate commercial child pornography by 2008. Our mission: to follow the money. First, we will aggressively seek to identify child pornography sites with method of payment information attached. Then we will work with the credit card industry to identify the merchant bank. Then we will stop the flow of funds to these sites.

In each case we will work hand-in-hand with federal, state, local or international law enforcement, and the first priority will be criminal prosecution. However, our fundamental premise is that it is impossible to arrest and prosecute everybody. Thus, our goal is twofold:

- (1) To increase the risk of running a child pornography enterprise; and
- (2) To eliminate the profitability.

We have created working groups of industry leaders to explore the best techniques for detection and eradication. NCMEC serves as the global clearinghouse for this effort, sharing information and working together in a truly collaborative way. We are grateful for the participation of international organizations and law enforcement agencies, such as the Serious Organised Crime Agency in the U.K. International cooperation is vital to our success due to the global nature of these enterprises.

Today I want to update you on the status of these efforts. We recently completed our pilot phase, from July 7 to September 9. We created a secure mechanism through which the information about illegal sites will flow between NCMEC, law enforcement, and the financial institutions. During this pilot phase the CyberTipline received 422 reports of commercial child pornography. NCMEC analysts viewed these sites and confirmed that the images were illegal. From these site analyses we identified 99 unique commercial child porn websites.

The names of these sites tell it all: "Elite Child Porn," "The Sick Child Room" and "Loli-Virgins." Each of these 99 websites offered multiple payment methods for the purchase of illegal images. We are seeing indications of a trend toward directing buyers away from credit cards and toward alternative payment methods to make the actual transaction. We are exploring possible explanations for this.

This pilot has given us a wealth of information that we could not have anticipated about the nature of these transactions and how to improve the flow of information necessary to identify the source of the images. We now know what we need to move into full implementation of the program. We need to capitalize on the investigative talents of multiple law enforcement agencies on a multi-national basis. And we need full participation by the payments industry worldwide. Then we will begin to dismantle these enterprises that profit from the heinous victimization of children.

Another project we recently began is the Technology Coalition, funded by AOL, Yahoo, Microsoft, Google, Earthlink and United Online. These industry leaders will work with NCMEC to develop and deploy technology solutions that disrupt the ability of

---

<sup>1</sup> Nilson Report, No. 849, 850, 851 (2006).

predators to use the Internet to exploit children or traffic in child pornography. The Technology Coalition has four principal objectives:

1. Developing and implementing technology solutions;
2. Improving knowledge sharing among industry;
3. Improving law enforcement tools; and
4. Research perpetrators' technologies to enhance industry efforts.

Bringing together the collective experience, knowledge and expertise of the members of this Coalition, and applying it to the problem of child sexual exploitation, is a significant step towards a safer world for our children.

Chairman Barton, you are the catalyst for our most recent initiative. You indicated an interest in the idea of a proactive effort to take down the child pornography websites that are not targeted by law enforcement for investigation. We have begun to work with major electronic service providers ("ESP") and the U.S. Internet Service Provider Association ("USISPA") towards the goal of making it more difficult to be able to access these sites. Our current partners in this effort are AOL, Microsoft, Google, Earthlink and United Online.

NCMEC analysts will identify child pornography websites that were reported to us without additional information that would permit a referral to a law enforcement agency. After we confirm the presence of illegal images on a site, we will add it to a list which will be provided to those ESPs who report to the CyberTipline. They will then take down the site and block its future access over their systems using filters.

We are actively working toward the implementation phase of this project and will keep you updated on our progress.

Another obstacle we are struggling to overcome is the fact that research indicates that most of the American public doesn't know about the CyberTipline. Reporting of child pornography and online enticement of children should be easier and more universal. We are eager to work with the industry to explore alternative reporting mechanisms, such as a link on the screen that enables reporting at the moment the illegal conduct is detected by the public.

The recent attention to child modeling websites raises the issue of whether some of these sites mask the true, illegal nature of their content. We want to stop these insidious sites that hide behind purportedly legal businesses to trade in images of sexually exploited children. We look forward to working with you and your staff to attack this problem as well.

The National Center for Missing & Exploited Children is grateful for your support, Chairman Whitfield, and that of your colleagues, in our efforts to protect children.

Thank you.

MR. WHITFIELD. Mr. Plitt, you are recognized for your 5-minute opening statement.

MR. PLITT. Thank you. Chairman Whitfield, Ranking Member Stupak, and distinguished members of the committee; thank you and good morning. With your permission, I would like to go ahead and submit the written testimony and just touch on a couple of issues very quickly. First is, the close cooperation across all lanes, government, private, NGO, is an absolute imperative. While the men and women of ICE, U.S. Immigration and Customs Enforcement, are honored to serve as the Nation's principal Federal criminal investigators for child exploitation and related financial crimes across the border, we

understand that cooperation and team work between all of us is essential to cover this enormous area of criminal activity.

This team work includes our partners in State and local enforcement, as well as the NGOs. While Federal law enforcement focuses on the interstate and international child exploitation crimes our State and local partners arrest the majority of child abusers and save the majority of the children. Special agents are grateful for the many prosecutors, companies and NGOs whose work is invaluable. NGOs, such as the National Center for Missing and Exploited Children, and initiatives such as the Financial Coalition Against Child Pornography help all of us in law enforcement coordinate and target our resources against the greatest criminal threats.

The NGOs provide countless solid leads, and the investigator-prosecutor relationship turns those investigative leads and our evidence into the seizures and convictions that are necessary. Prosecutors' speed and willingness to reach out to their colleagues across jurisdiction is vital in the investigation of Internet crimes against children. Rapid response to ICE requests for help by Internet and financial service companies are deeply appreciated. Second, Internet child pornography is a big business. As far back as 1992, ICE, then the U.S. Customs Service, investigated the sale of access to Internet bulletin boards containing images of child abuse, which in one investigation was shown to generate more than \$60,000 per month in proceeds.

Five years later in 1997, another ICE customs investigation revealed that proceeds from the sale of access to child exploitation websites can easily exceed \$1 million a year. In the 1999 landslide investigation, we uncovered that the magnitude of illegal revenue derived from the sale of access to child exploitation websites was occurring still at that level. ICE addressed the trans border aspect of the landslide investigation in support of the Dallas Internet Crimes Against Children Task Force, and of course other Federal partners, the U.S. Postal Inspection Service, as well as the FBI. Four years later, ICE seized approximately \$800,000 in the 2003 Operation Falcon RegPay case. Currently, open investigations continue to demonstrate the big money behind this activity.

Third, advances in the Internet and due to technology they are making it difficult to identify and track the global financial infrastructure that facilitates Internet child exploitation businesses. Our laws, the tools that we in law enforcement use to fight these crimes are not keeping pace with the continued evolution of digital money. These digital monies move around at the speed of light and with a click of a mouse. I would also like to indicate that while the focus today is on child exploitation crimes and the illegal financial transactions that support them, these same mechanisms, these same Internet mechanisms, are being used for

other Internet crimes be it property right violations, pharmaceuticals, as well as the sale and distribution of false identity documents.

In conclusion, on behalf of the men and women of ICE, I wish to express our gratitude to the subcommittee for continuing this series of hearings and to the important issue. In this area, we face massive amounts of criminal activity. Collectively, we understand the challenge that we face, and we need to study it more. We need to understand the trends, the techniques, the vulnerabilities of those engaged in these international criminal business enterprises, and Congress has a vital role in insuring that law enforcement has the tools it needs to keep pace with these criminal activities and the way that these criminals seek to hide within the cutting technology Internet and computers. Thank you again for this hearing, and I stand by for your questions.

[The prepared statement of James Plitt follows:]

PREPARED STATEMENT OF JAMES PLITT, DIRECTOR, CYBER CRIMES CENTER, OFFICE OF INVESTIGATIONS, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

#### INTRODUCTION

Chairman Whitfield, Ranking Member Stupak, and distinguished Members of the Energy and Commerce Oversight and Investigations Subcommittee, my name is James Plitt and I am the Chief of the Cyber Crimes Center at the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE). I appreciate the opportunity to present an understanding of ICE's authorities and responsibilities with respect to investigating international commercial child exploitation websites.

#### THE COMMERCIAL ONLINE CHILD EXPLOITATION ENVIRONMENT

The ICE Cyber Crimes Center (C3) is responsible for investigating violations of immigration and customs laws that occur in cyberspace, including trans-border sexual exploitation of children over the Internet. When ICE investigates the online sexual exploitation of children, we focus on three components of the Internet: international commercial and non-commercial websites, international Peer-to-Peer groups, and international Internet Relay Chat.

Criminal organizations increasingly use the Internet to internationally advertise, distribute, and receive electronic contraband, specifically images of child exploitation. In doing so, they are reaping enormous profits from the sale of access to websites containing these images. To stop the proliferation of international commercial child exploitation websites, C3 dedicates substantial investigative resources to identifying and dismantling the criminal organizations responsible for such sites and the exploitation from which they profit.

Although it is difficult to determine the exact number of websites offering images of child sexual exploitation, observations from ICE investigations generally support the statistics of non-governmental organizations like the National Center for Missing and Exploited Children, which estimates that more than 100,000 such websites exist, more than 1,000 of which are commercial in nature. Among members-only websites, there is a tremendously high rate of duplication, with many identical or noticeably similar sites operated by the same individuals. Furthermore, we often encounter 10 to 15 different advertising websites operated by the same individuals, all of which link to the same

members-only website. This renders an accurate count of websites depicting child exploitation especially difficult to obtain.

Recent investigations, including ICE's unprecedented Operation Falcon, have revealed a common methodology that criminal organizations use to commercially distribute images of child exploitation around the world. Typically, the organization consists of at least three component groups. The first of these groups includes the individuals responsible for uploading and maintaining the advertising and payment websites. These websites provide willing customers the opportunity to purchase Internet access to websites with a large volume of child exploitation images. The second group consists of individuals who facilitate the payment process. ICE has identified the following online payment methods used by international commercial child exploitation organizations: e-Gold, PayPal, Western Union, and traditional credit card-based merchants. We believe there are subgroups within this second group with responsibility for exploiting each type of international Internet payment method. They remain attentive to the development and availability of new financial methods. The third group consists of those who control the overall criminal organization, decide which payment method will be used in a given situation, determine the content of the members-only child exploitation website, and direct the laundering and distribution of the proceeds.

ICE's Internet child exploitation investigations have revealed that many of those who control and profit from these electronic images are located in Eastern Europe and former Soviet countries. Furthermore, there is likely some overlap within these organizations because of the ease with which the three groups described earlier can provide their services to multiple organizations at any given time. For example, an organized payment facilitator can easily accept payments from multiple advertising websites for access to multiple members-only websites. A website that advertises access to members-only child exploitation websites is easy to upload to Internet web servers and can be operational at multiple locations within one day. Payment websites have a similar structure and are easy to operate, whereas members-only websites are much larger and more difficult to upload. Generally the same members-only website is uploaded on one Internet web server and allowed to operate for 30 days, after which its operators remove it from the server and upload it to a different server.

#### CONCLUSION

C3 is dedicated to identifying all individuals involved in international criminal organizations and component groups that conduct every activity associated with international, commercial child exploitation websites. This includes those who advertise specific members-only websites, those who facilitate customer payments, those who control the members-only websites, and those who ultimately receive the proceeds from the sale of child exploitation images. With our expertise in money laundering investigations, we are working diligently to identify and dismantle the international criminal organizations that operate these commercial child exploitation websites, as well as to identify their many subscribers. ICE coordinates closely with the Internet Crimes Against Children Task Forces, various elements of the Department of Justice's Project Safe Childhood initiative, and non-governmental organizations like the National Center for Missing and Exploited Children to maximize the effect of these international investigations and thereby protect this nation's most valuable resource, our children.

I hope my remarks today have been helpful and informative. I thank you for inviting me and I will be glad to answer any questions you may have at this time.

MR. WHITFIELD. Thank you, Mr. Plitt, and I appreciate the testimony of all three of you. Mr. Christie, let me first begin with you.

The RegPay case, I am assuming, was one of the first and most comprehensive prosecutions in this entire area, is that correct?

MR. CHRISTIE. That is correct, Mr. Chairman, yes.

MR. WHITFIELD. And how long did that investigation go on including the actual trial, what was the time period?

MR. CHRISTIE. The investigations and trial went on for about 3 years, Mr. Chairman.

MR. WHITFIELD. And how many people were actually convicted, roughly?

MR. CHRISTIE. Roughly, across the country when you look at all of them there were probably about 200 or so that were convicted when you take into account also the users and the purchasers of the information as well.

MR. WHITFIELD. And this was a world wide operation?

MR. CHRISTIE. Yes, it was, sir.

MR. WHITFIELD. But it was headquartered in Belarus?

MR. CHRISTIE. The websites were headquarters and created in Belarus. The financial transactions occurred mostly in the State of Florida. Purchasers were all across the United States, and the money eventually sent to banks in Latvia.

MR. WHITFIELD. Okay. Now what lessons should be learned from the RegPay case in terms of how to investigate and ultimately prosecute these complex international commercial child pornography cases, what lessons did you learn?

MR. CHRISTIE. First and foremost is you have to have the cooperation of the credit card companies by providing this information on a real time basis, and one of the things that we did in the RegPay case was to go to the credit card companies up front early in the investigation and say to them we want your cooperation in terms of giving us this information on a real time basis so we can trace these transactions. That has not always been the way it was, but I have to say that we had enormous help from MasterCard and Visa who were willing to do things that really had not been done before in these investigations in terms of providing us with that information.

So that is one. You need the cooperation of the credit card companies to be able to do this. They are the gateway into this. I think the second is to make sure that all of the law enforcement agencies involved are on board and ready to cooperate internationally. You have to reach out to your international partners. You need them to be a part of the group and they certainly were in the RegPay case. And I think the third thing that we learned from the investigation was that you can have success doing this. Now part of getting law enforcement interested in devoting the time of enormous resources that we need to devote to be

able to bring this down is hopefully to have prosecutions at the end of the day, not to have it lead to a dry hole and lead to frustration.

And what we proved to all the other districts in the country is that you can do this and you can succeed and you can get these folks, the really bad people, who are exploiting these children. And as I said before, Mr. Chairman, the images that were on this website were incredibly disturbing and exploitive of children. You had child rape scenes and just the worse things that you can imagine in children as young as 5 and 6 years old.

MR. WHITFIELD. Were these on demand?

MR. CHRISTIE. Well, no, these were not live shows but they were depictions of photographs that had been taken and that these people could get. And the other point that was brought up before that is something that we are going to need to confront is when people don't pay with money for these images. We are seeing an increase in the uploading of pictures so there is ways to join these sites and have memberships in these sites, and one of the ways is to pay, but the other way is to say if you are willing to upload to the site a certain number of new child pornographic images, that can take care of your membership fee for a certain period of months or even years depending on how many of these images you have.

So what that is creating is cottage industries of people who want to create these images as a way of not having to pay to see other images but create their own images to upload, and that phenomenon is something that we are very concerned about as well. So we are focusing on that as well so not to look at the users anymore. It is just people who are sitting and clicking a mouse and looking at an image, but also to see them as potential active pedophiles to try to support their need for further stimulation by getting these other images.

MR. WHITFIELD. Thank you. Mr. Allen, you had mentioned in your testimony that 80 percent of the payment processors had joined your coalition to deal with this issue. Of that 13 percent that did not join, did they give you any particular reasons for not joining or was there a theme of why they were not interested?

MR. ALLEN. No, Mr. Chairman, there is really not. We have had an aggressive recruitment effort, but there are a lot of people in the financial industry in this country. For example, I just learned this morning of another company because of your hearing who wants to be involved, so we just got to try harder and work harder, and I think frankly the kind of diversity of financial leadership that is represented here should reassure these companies that this is not a risky thing to do, this is the right thing to do. It is not only good for the country but it is good for them.



MR. WHITFIELD. Absolutely. And, after today we are going to have the Chairman of e-gold, which is a digital currency company. Now you are a real expert in this whole area relating to child pornography, and you have done a great job of setting up this national center. What sort of problems does this digital currency present as you try to identify child predators and pornography?

MR. ALLEN. Well, I think our concern initially was that as you put pressure on the mainstream payment systems the most likely thing that would happen is they would move to alternative payments, and that is one of the reasons why one of the first people we talked to about involvement in this coalition was Dr. Jackson at e-gold, who has been a part of this process, and has been very aggressive in our judgment in trying to root this out. Similarly, the other alternative payment mechanisms have been similarly aggressive. What we are seeing now, I think, and Mr. Plitt and others could speak more accurately to that than I, is a kind of continuing evolution. As you put pressure on one point, they move somewhere else so we are now seeing the development of small aggregators and almost customized payment mechanisms.

But I think there is no question that if we are successful, we are going to keep them moving into new payment devices and we are going to get them out of the sort of mainstream payment systems.

MR. WHITFIELD. So did Dr. Jackson agree to work with you to?

MR. ALLEN. Yes, he did, and has.

MR. WHITFIELD. Okay. Now, Mr. Plitt and Mr. Christie, would you all like to expand on this digital currency and the problems that that creates?

MR. PLITT. Yes, absolutely. The digital currency methods are evolving daily. As I mentioned in my 5-minute opening, it is moving into areas besides just child exploitation so you find that the digital currency is becoming a substrate for Internet activities. The only other thing I would like to mention at this point is that the focus is on the payments associated with joining a commercial child exploitation website. I would also ask the committee to consider that on the back end of that the proceeds that are derived from that activity are also resident on the Internet. They don't necessarily take the money out as cash or move it to some legitimate bank account. It can stay on the Internet and those e-currencies, those currency devices, can be bartered for services that support those websites such as content.

MR. WHITFIELD. Okay. Mr. Christie.

MR. CHRISTIE. I would agree with what Mr. Plitt said. What it is creating for law enforcement is additional challenges. As you knock down one area another one pops up some place else because you need to understand, I know this committee does after the work that you have all

done, the incredible scope of the money that is being made here. Billions of dollars are being made. And so people are not just going to quickly abandon that. They are going to use their best and brightest to try to work against us as we attack and defeat one area, and so we have to continue to remain very nimble.

And I think the work of this committee in drawing all these different institutions together is going to be very helpful to get information to everybody on how we can remain at least even with them if not the goal of getting one step ahead of them and stopping them before they innovate. But it is an enormous challenge because of the resources that they bring to bear. Mr. Plitt is right, they use those resources as a barter system on the Internet to support their information. That makes it very difficult for law enforcement to trace those proceeds.

MR. WHITFIELD. In my understanding the digital currency is not regulated in any way by the Federal government, is that correct?

MR. CHRISTIE. Correct.

MR. WHITFIELD. At this time right now is Mr. Stupak.

MR. STUPAK. Thank you all for coming. You know, you were just talking about knocking down sites and another one pops up, Mr. Christie. Mr. Allen, you were telling us last time when you testified about Great Britain, how all their ISPs from a coalition, and they have dropped like in 2 years sexual exploitation from 18 percent down to .04 percent. Now is that a trade association within Britain that helps monitor this? Explain that to us.

MR. ALLEN. It is the Internet Watch Foundation. It is a non-profit, non-governmental organization that is basically sustained through revenues that come through the companies. Let me say we have great admiration for them. We have included them in our meetings. We have skepticism about the data. We still identify--

MR. STUPAK. But it is better than what we are doing in this country, right?

MR. ALLEN. Well, I think what we are trying to do is to adapt it. The step we are taking here, I mean our concern is that blocking is not enough.

MR. STUPAK. I agree.

MR. ALLEN. Yeah. Okay.

MR. STUPAK. But could we do things similar to what they are doing in Great Britain to make it--as Mr. Christie says we shut down one, another one pops up, we all know. What do we have, about 1,300 ISPs at least in this country?

MR. ALLEN. At least.

MR. STUPAK. Okay. So have any of them joined an Internet Watch like they do in Great Britain?

MR. ALLEN. No. I think the step we are trying to take here is attempting to emulate that so that all ISPs in this country are required to report child pornography on their systems to us. As we discussed at the last hearing, there are still some issues regarding getting everybody to do that.

MR. STUPAK. Correct. The Department had some concerns about a law Congress passed even though they never used the law to accuse but they already--okay. Mr. Christie, one of the other concerns were--you were involved with RegPay, right?

MR. CHRISTIE. Yes.

MR. STUPAK. And I noticed in the testimony about you had to do search warrants for Connections. This was a company in Fort Lauderdale that the money went through, correct?

MR. CHRISTIE. Correct.

MR. STUPAK. What problems or one of the concerns of law enforcement it takes too long to get a search warrant and they talk about an administrative warrant. Have you seen that problem in RegPay that took too long to get search warrants to have them be beneficial?

MR. CHRISTIE. Congressman, I did not see that problem in RegPay. I think that is because we have developed so much probable cause so quickly that I did not see the problem in the RegPay case in terms of the speed of us getting our search warrants, and so it was not something that we experienced in the RegPay case as a problem on that specific case. There may be other instances when that occurs in other districts, but in our district in that case we did not have that problem.

MR. STUPAK. One of the problems I did see in that one was trying to get these people who were responsible here for this to come to another country where they were arrested and all that because they were from Belarus which didn't handle that. In this case, RegPay or was it Operation Falcon, I think, was another word for it?

MR. CHRISTIE. Yes.

MR. STUPAK. If there were 21,000 distinct purchasers of child pornography off that site, that is here in this country and we prosecuted less than 500. I have been told that the Australians have prosecuted about 600 out of 900 to date, and the Dutch have told our staff that they have prosecuted 629 out of 640. So my question is from a prosecutor point of view why are prosecutions so low out of those 21,000?

MR. CHRISTIE. Well, I think part of it is obvious from the numbers. To give you some example, our office, which is one of the larger U.S. Attorney's offices in the country, we have about 135 Assistant United States Attorneys, we prosecute to a conclusion on an average year somewhere between 800 and 900 cases. So if you look at the numbers that you are talking about with 21,000 purchasers the idea of any one or

even a combination of all 94 U.S. Attorney's offices being able to prosecute the kind of percentages that you are talking about and comparing to the other countries when you have 21,000 purchasers it would simply overwhelm--it would overwhelm our ability to do anything else.

And so what we have tried to do with our law enforcement partners is to target those folks who have potential for direct contact with children on an every day basis, people who are involved in schools and religious organizations, et cetera, and so we certainly make choices regarding who we pursue and how we prioritize that.

MR. STUPAK. A figure that sticks in my brain because you were talking about--this is our sixth hearing, those people in there, 80 percent of them are abusing the people, child pornographers who view this stuff, a lot of them will abuse their own children or other children so wouldn't this be a higher prosecution priority of these 21,000? And also I didn't expect all 94 U.S. District Attorney offices to prosecute. Why wouldn't you just turn them over to State and local prosecutors to get a better percentage?

MR. CHRISTIE. Well, there are some instances where it is appropriate to give those to State and locals, and we do. But as well I am unsure of the 80 percent number that is used, and that seems higher than what I have been familiar with before of people who are proven pedophile abusers who are also viewing this information. I will tell you, Congressman, it is a very high priority in our district and the resources that we have placed on it. I have nearly 10 percent of all my Assistant United States Attorneys in my office who are working on child pornography, so when you look at the full plate of things that we have to deal with in the United States Attorney's Office of our size, we are placing a high priority on this and moving as many of these cases as we possibly can.

MR. STUPAK. Of these 21,000 then if they are from let us say Michigan were the prosecutors, State and local prosecutors, then notified of these people?

MR. CHRISTIE. Sure. What happens is--

MR. STUPAK. And then it would be up to them?

MR. CHRISTIE. These leads go out through ICE to all their places, all their different offices across the country. They are given to both the U.S. Attorneys offices and to their local law enforcement partners. And so all those leads of those 21,000 are distributed to law enforcement throughout the country. They are not ignored, but the question is when do the statistics catch up and in what percentage can all these people do these cases?

MR. STUPAK. Do you follow up on these 21,000? I would really be interested to see when they do catch up because I would be interested in knowing those numbers.

MR. CHRISTIE. I think ICE probably is the focal point for following up on those leads as they are the lead investigative agency. We certainly keep up with the ones that occur in New Jersey, but then once we gather all that information as the lead U.S. Attorney's Office in the country on a case like RegPay or Falcon, we turn to ICE to distribute those throughout the country, and they are really the ones who follow up on those statistics across the country.

MR. STUPAK. Could you get that information for us? Mr. Allen, you indicated that 87 percent of financial institutions have joined your financial coalition, I believe you called it. How do we persuade the last 13 percent to join?

MR. ALLEN. One at a time. That is exactly what we are trying to do. And I think frankly one of the greatest successes we have had is that companies that are part of this coalition are going to their competitors and colleagues and saying you need to be a part of this.

MR. STUPAK. Thirteen percent. How many in a raw number? What would that be of financial institutions that have not yet participated or not trying to help in this financial coalition? Do you have a raw number?

MR. ALLEN. I can get that for you. My sense is it is a fairly large number.

MR. STUPAK. Right, that has been my sense.

MR. ALLEN. Once you get past the big guys then the rest, that 10, 12 percent involves a lot of small institutions, many of whom probably don't think they have any relevance or connection with this.

MR. STUPAK. Okay. So the big ones really--e-gold is part of your financial coalition?

MR. ALLEN. Yes.

MR. STUPAK. And Western Union?

MR. ALLEN. Western Union is not.

MR. STUPAK. I was looking at some of the documents you gave us, confidential ones, and some of them had Western Union on there to further the financial transactions.

MR. ALLEN. One of the challenges there and one of the reasons that Western Union sometimes is used, is if the transaction is less than \$1,000 there is no information about the sender or the distributor. So that is--first data which I believe is the parent of Western Union, I think that is right.

MR. STUPAK. But a lot of these sites also say on there if you use like MasterCard and Visa, and I am trying to find this one right here, some of them where I had it marked, basically say your name and address will not

be disclosed. Everything is confidential. That is not necessarily true if you use a MasterCard or Visa or something like that. There would be a way to erect that transaction, right?

MR. ALLEN. That is exactly what we are trying to do.

MR. STUPAK. We have had other hearings in Oversight and Investigations through my years on this committee, and I think, Mr. Plitt, you mentioned that identity theft, pharmacy, drug masking agents, would your financial coalition model work to help stop the drug masking, things being sold through the Internet, credit card companies, Internet pharmacies that are not proper, identity theft, do you think your model would work for other products, if you will?

MR. PLITT. Congressman, I don't know why not. I mean I think it is a great model because private industry competitors are coming together, exchanging information, working with law enforcement to address the financial aspects of this. I think it is too early to say that this model works but certainly my sense 6 months in is that it is a great model that could be replicable in many ways.

MR. STUPAK. Thank you.

MR. WHITFIELD. The gentleman from New Jersey is recognized.

MR. FERGUSON. Thank you, Mr. Chairman. Mr. Christie, my understanding is that over a thousand arrests came from the information from the RegPay case, both domestically and internationally. That is a huge number. We know it only really begins to scratch the surface of this problem. You have talked about the enormous resources that your office devotes to this particular type of activity. What are the--the title of today's hearing could easily be called follow the money. We are examining that aspect of it today. What challenges, if any, did you see in the RegPay investigation that we could learn from your work with, specifically regarding the financial institutions because you have set up the model.

This should be hopefully the template for other law enforcement to be able to use to be able to track down these folks that are doing this. Were there any challenges that you experienced in the process of that specifically with regard to the financial institutions that we could help to address or that we could try to remedy?

MR. CHRISTIE. Sure. The first one, Congressman, is to have buy-in from the credit card companies to be up front providing real time information to law enforcement so that we can trace these transactions to the processors and the people who are laundering this money for the people who are setting up these pornographic websites. And in the RegPay case we were able to get voluntary buy-in from MasterCard and Visa in what I think one of the first times that happened on a real time basis. And we went and made the pitch to them and they cooperated.

And so that is very important, and I don't think you can do one of these investigations without cooperation from those credit card companies. It is absolutely vital since still the overwhelming majority of these transactions are processed in that way.

Secondly is to make sure that you have the type of trained investigators that you need to follow this. This is not easy stuff. It is very complex. And so to make sure that ICE has the type of agents and more of those agents that can trace this type of money trail, have the training and the expertise to do that. We also utilize the IRS in this regard and that investigation was a partner with ICE. And the IRS has enormous expertise for obvious reasons in following the money trail, and they worked in partnership with ICE and RegPay and Operation Falcon to be able to do that.

And so making sure that those agencies have the type of trained investigative personnel in greater numbers than they have now if we want to try to become even more aggressive about this because we as prosecutors can't do these cases unless the evidence trail is built, and it is built by these investigators who work enormously hard on very, very complex transactions because, as you know, these folks don't want to be caught so they make these transactions as complex as they can in an effort to try to frustrate us off of their trail.

So I think those are the biggest lessons from a financial prospective. We learned we need to continue to build up the expertise within ICE and IRS across the whole country to be able to partner with the U.S. Attorney's Office and local law enforcement to go after these transactions, and we also need to make sure that all the people in the financial industry are committed to working with law enforcement on a real time basis to get us the information we need to be able to get after these child predators.

MR. FERGUSON. Now the gentleman from your office who prosecuted the RegPay case, Carlos Ortiz, is that correct?

MR. CHRISTIE. Yes.

MR. FERGUSON. He is currently in private practice?

MR. CHRISTIE. Yes, he is.

MR. FERGUSON. No longer works in your office?

MR. CHRISTIE. No, he no longer works for me.

MR. FERGUSON. Well, please give him our best and our thanks if you happen to see him.

MR. CHRISTIE. I speak to Carlos on a regular basis. He is still very involved with Mr. Allen in his private capacity at the National Center advising them on these issues, and so we speak frequently and he is a good friend.

MR. ALLEN. Congressman, could I interject? Carlos Ortiz is providing legal counsel to our financial coalition through his law firm in New York on a pro bono basis so that is how committed he personally is to this whole effort.

MR. FERGUSON. Mr. Plitt, could you follow up on what Mr. Christie was talking about in terms of the financial institutions and cooperation that you may have received, and speak specifically--I don't like to harp on the problems. If someone is doing the right thing, we like to recognize that, but are there problems, are there road blocks that you are running into, are there things that we can be doing or working on together to encourage folks to be more cooperative

MR. PLITT. Yes. We are getting considerable cooperation from various financial companies, banks, credit card companies, et cetera, so I think their heart is in the right place. But this type of crime and the use of the financial systems and the new financial systems, the Internet financial systems is causing a lot of people to learn different things and it takes a while to come up that learning curve. And just when we get to the point where we have a great template like the RegPay case it shifts to new methods. For instance, we are seeing steward value cards. We are seeing non-credit card based financial transactions used to join these as members to these websites.

So they are learning as fast as we are. Obviously, I would think that the financial companies are interested in protecting their own assets, their own portfolio of customers so it is of value to them, but from what I hear from our investigators the speed with which the information is provided to us, the desire to learn with us as we work the investigations is very high, very appreciated.

MR. FERGUSON. Mr. Allen, thanks again for all of your work and your staff's work at the center. As you know, I spent an afternoon over there one day and as horrifying as it is to see the job that you and your team are doing every day we are so thankful that you are doing it, so thanks for that. That goes, of course, for Mr. Christie and Mr. Plitt in your work as well. You talked about the kind of coalitions and the round tables or I forget the exact term you used for the way you are bringing people together, both ISPs and the folks in the financial world. Are you--obviously you are getting a good bit of cooperation and you come from a gold-plated organization. You would think someone was crazy not to step up to help. But are you getting the cooperation that you feel like you need from all the players here or are there folks that we need to continue to work with or encourage?

MR. ALLEN. Well, yes, the answer is yes. I think we are getting great cooperation certainly from Federal law enforcement. I do want to second what the Chairman said in the beginning regarding the need for



more law enforcement resources in this area. I was very enthusiastic about Mr. Stupak's proposal to increase the resources for Mr. Plitt and our friends at ICE. We are getting great cooperation from these financial companies, and I really think this is an unprecedented approach because they are working collaboratively. These are fierce competitors in the day-to-day world. Where we need help, as I said in my testimony, is I think this is something we are shining light on the problem and putting pressure on these companies that are not a part of this effort is important. I think putting pressure internationally is important. One of the things we have learned, our international center reviewed the law, the statutes, in the 184-member countries of Interpol, and we found that in 95 of those countries child pornography is not a crime. There is no law.

So in most of the countries that are member nations of Interpol, this problem, a global phenomenon, is not even against the law. So we have a lot of work to do internationally, and the reason that your hearings have been important and the actions that you have taken are so important is that despite the fact that this is a multi-national problem, despite the fact that the Internet is a global phenomenon, I remain convinced that the vast majority of the consumers are Americans. We just spoke with a Russian legislator trying to push legislation in Russia on this issue and she said to us we will propose the legislation but you need to do something about the demand because the demand is American so there is a lot more that needs to be done.

MR. FERGUSON. Similar in some ways to the scourge of drugs, drug use.

MR. ALLEN. Absolutely.

MR. FERGUSON. Just before my time is up, Mr. Allen, but with the coalition that you announced and have talked about to filter sites, you explained that the site information is given to law enforcement before it is given to ISPs to block. Does law enforcement have the option in terms of asking the ISPs or asking you all to keep the site up for investigation purposes? As horrible as that sounds, you can imagine a scenario where that might actually be more useful in being able to gather information in terms of looking at down the road. Is that option available?

MR. ALLEN. I obviously don't want to reveal investigative details, but I think that has long been a practice because as was discussed earlier developing the necessary investigative information is the case, and it is certainly one of the things that we have grappled with in our financial coalition process is how do you balance the two. These companies want to act immediately. Law enforcement wants to have an appropriate amount of time to determine whether they are going to proceed with formal investigation, and the tension is to find the middle ground. So the answer generally, Congressman, is yes.

MR. FERGUSON. Thanks, Mr. Chairman.

MR. WHITFIELD. The gentleman's time has expired. We have three votes on the House floor. We have still about 5 minutes before the first vote is over, and so Ms. DeGette is going to be delayed getting back so I am going to recognize her to ask a few questions.

MS. DEGETTE. Thank you so much, Mr. Chairman. I will be delayed and I won't be able to fully ask this panel questions, but I want to thank all three of you for your hard work. Mr. Plitt, we have seen you before. I just want to ask the three panelists what their opinion is about the idea that I have been talking about which is requiring the ISPs to retain the identifying data for a 1-year period. Do you think that would help with law enforcement techniques? Mr. Christie, we will just start with you.

MR. CHRISTIE. Absolutely, Congresswoman, I think retaining that data is very important, and it helps to give us the option to be able to really follow these trails fully to the end. If that information goes away, it makes it much more difficult for us. And so my own opinion in terms of having been at the front of one of these investigations is we need more and more information and we need it as quickly as we can possibly get it because how quickly these sites evolve and change, so it would be helpful.

MS. DEGETTE. Mr. Allen.

MR. ALLEN. Yes, and it is a difficult issue. What we like about your proposal is that you are not talking about retaining content. What our focus has been is sort of the connectivity law. The reality is that law enforcement has to be able to connect the images that are identified to a particular person and a particular address, and I think that connectivity aspect is critical. Obviously, this is a real dilemma for the ISPs for a host of reasons, and I think there is an appropriate time frame that can be established. But overwhelmingly we think this is something that law enforcement needs to have.

MS. DEGETTE. Mr. Plitt.

MR. PLITT. Yes, the data retention is something that is absolutely necessary. The two enemies in Internet investigations are time and data volume, and with respect to time I think what we would find that looking at the 21,000 targets shall we say from the RegPay Falcon case unfortunately the information wasn't available so the staleness of probable cause, staleness of information, is a large matter.

MS. DEGETTE. And I assume though you wouldn't use a 1-year law as an excuse to drag your feet in investigations in any way?

MR. PLITT. Oh, no, no. We work the cases as quickly as we can. These are high priority cases for us.

MS. DEGETTE. Thank you. Thank you very much, Mr. Chairman, for your accommodation, and thanks again to the panel.

MR. WHITFIELD. Thank you. As I said, we have three votes on the floor. There is about a minute left on the first vote and then there will be two 5-minute votes, so it will be our goal to be back here by 10 till 12:00--no, 5 till 12:00 or 12:00. That is our goal. And then we have additional questions for the first panel, so we will recess until about 5 minutes till 12:00.

[Recess]

MR. WHITFIELD. The hearing will come back to order. We are waiting for a couple other members but in the meantime Mr. Stupak had a couple of additional questions that he would like to ask, so I will recognize Mr. Stupak.

MR. STUPAK. Thank you. Mr. Plitt, if I may, I asked Mr. Christie about search warrants. Do you find search warrants in these cases problems, take too long, evidence goes cold on you? What has been your experience in that area?

MR. PLITT. In the first few types of these cases it was an educational issue for the prosecutors as well as the agents. We have worked through that. And I will tell you something that is underway is working through Project Safe Childhood. We are working to establish the attorney in that area in that particular jurisdiction who would be able to respond to exigent search warrant situations, so we are already looking at some of that. Other than that, not too many problems.

MR. STUPAK. So a regular search warrant or administrative search warrants, what type would you be seeking?

MR. PLITT. We would usually seek criminal-based search warrants.

MR. STUPAK. And it is not a problem?

MR. PLITT. It hasn't been a problem, that is correct.

MR. STUPAK. Very good. I have no more questions, Mr. Chairman.

MR. WHITFIELD. Well, I want to thank the first panel for being with us this morning. We genuinely appreciate your testimony and the information you have provided, and we look forward to continue working with you as we make efforts to make a continued dent into this problem. And with that, I will release the first panel. Thank you very much. At this time I would like to call up the second panel, and are we going to have a second panel, by the way? Okay. We originally on the second panel had a John Doe testimony from a Federal corrections institute, and that still has not been decided completely, so at this time I would like to call up the third panel.

And on the third panel we have Mr. Arne Christenson, who is Senior Vice-President, Federal Government Affairs with the American Express Company. We have Ms. Jodi Golinsky, who is Vice President and

Senior Regulatory Counsel for MasterCard International. We have Mr. Joe Sullivan, who is the Associate General Counsel of PayPal. We have Mr. Mark McCarthy, who is Senior Vice President, Public Policy, for VISA. And then Mr. Douglas Jackson, who is the Chairman of e-gold Group, and we would invite him to come up and testify as well.

I want to thank all of you for being with us today. Of course, this hearing is really focused on this panel, and we know that you all have taken many steps to assist in the significant issue that we face. As you recognize, it is an Oversight and Investigations Subcommittee hearing, and we do normally take testimony under oath. Do any of you have any objections to testifying under oath? If not, then if you would please stand and raise your right hand, I would like to swear you in.

[Witnesses sworn]

MR. WHITFIELD. Thank you very much, and all of you are under oath now. Mr. Christenson, we will recognize you for your 5-minute opening statement.

**TESTIMONY OF ARNE L. CHRISTENSON, SENIOR VICE PRESIDENT, FEDERAL GOVERNMENT AFFAIRS, AMERICAN EXPRESS COMPANY; JODI GOLINSKY, ESQ., VICE PRESIDENT AND SENIOR REGULATORY COUNSEL, MASTERCARD INTERNATIONAL, INC.; JOE SULLIVAN, ESQ., ASSOCIATE GENERAL COUNSEL, PAYPAL, INC.; MARK MCCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA U.S.A., INC., AND DOUGLAS JACKSON, CHAIRMAN, E-GOLD GROUP, INC.**

MR. CHRISTENSON. Thank you, Chairman Whitfield. Chairman Whitfield, Ranking Member Stupak, my name is Arne Christenson. I am a Senior Vice President at American Express for Federal Government Affairs, and I also serve as our company's representative on the Financial Coalition Against Child Pornography. And we at American Express are proud to be working with the National Center and our colleagues in the industry on that important effort. It is a privilege to testify today about our efforts at American Express to block any use of our cards to purchase child pornography on the Internet.

Today I would like to just briefly describe our business model, and then list the steps we take so that our network is not used to fund child pornography and outline what we are doing to focus even more intensely on combating this evil in the future. American Express was founded in 1850 and is today a diversified worldwide company focused on payments, travel, and financial services. We operate what is often referred to as a closed loop network, which is distinguished in some

ways from major networks like Visa and MasterCard. In an open network model the networks process transactions and serve as a connecting point between an acquiring bank which has the relationship with the merchant, and an issuing bank which has the relationship with the cardholder. At American Express, all these functions take place within one company. We issue cards to customers. We operate the network, and we manage the relationship with merchants who accept our cards.

Consequently, our work to combat child pornography involves activities that may be undertaken by two or three different entities in the open network model. We screen merchants who wish to accept American Express as an acquiring bank might do in the open network model. We track activity on our network constantly to ensure that merchants are not violating our policies, as Visa and MasterCard do, and we work with law enforcement to respond to any potential illegal activity on our network, whether that activity involves cardholders, merchants, or both.

Let me say, first of all, a few words about our due diligence. We restrict or prohibit the signing of merchants that fall within 16 general categories. First and foremost, we do not accept merchants that are linked in any way to illegal activities, including child pornography. In addition, since 2000 we have had a broader ban on Internet pornography in general. When a merchant wants to begin accepting the American Express card, we look at a number of different things, their financial records, their past history with us, their past history with other card networks, any websites they might have, and merchants that we view as a higher risk are routed to an internal contract review team for further investigation.

We decline thousands of merchants every year because they do not meet our criteria. In addition to this review at the time of signing, we continually monitor merchant submissions to identify suspicious activity or patterns that are not consistent with the merchants identified industry. In doing so, we identify and investigate transactions that differ in important ways from what would be customary or expected for a particular merchant. In the case of Internet merchants, we also conduct ongoing monitoring of the World Wide Web to detect any violations of our policies.

Our Web crawlers review millions of Web pages each day, and in the case of child pornography this search includes proprietary technology designed to detect such sites. When we discover merchants who are violating our policies, we can take immediate action and terminate them. By every indication our policies and procedures have effectively blocked the use of our network to finance child pornography. In cases where we

have found a website that could be linked to child pornography, we have terminated the merchant. However, the vast majority of merchant cancellations in this area stem from violations of our broader policy on Internet pornography.

The statistics on the National Center are consistent with these findings. In 2005, a very small percentage of all commercial child pornography referrals received by NCMEC contained references to American Express. Our own experience indicates that very few of those sites that mention American Express would actually connect to a merchant on our network. While our research shows that very few child pornography sites take our card, it appears that they often promote payment by credit cards to make the site appear more legitimate. Indeed, there is a growing trend toward steering visitors of these sites to various alternative payment methods.

While our restrictive rules have been broadly effective, we are focused on two areas where we believe we can do more to be more effective. First, we have changed our process for monitoring the Internet. In the past our search for child pornography sites took place as part of our broader efforts to enforce our Internet pornography and there was not a clear differentiation between the two in our review and reporting. We now separately track and, if necessary, refer to law enforcement any sites that could include child pornography.

Second, through our work with the Financial Coalition, we have instituted a more effective, documented, and ongoing consultation with law enforcement on child pornography issues. American Express is committed to working in partnership with law enforcement and others in the industry to deny child pornographers access to the payment system, and we appreciate your focus on this important issue. I would be happy to take questions.

[The prepared statement of Arne Christenson follows:]

PREPARED STATEMENT OF ARNE L. CHRISTENSON, SENIOR VICE PRESIDENT, FEDERAL  
GOVERNMENT AFFAIRS, AMERICAN EXPRESS COMPANY

Chairman Whitfield, Ranking Member Stupak, distinguished members of the Subcommittee, my name is Arne Christenson, and I am a senior vice president at American Express responsible for Federal Government Affairs. I also serve as our company's representative on the Financial Coalition Against Child Pornography.

American Express Company was founded in 1850 and is today a diversified worldwide travel, network and financial services provider. We are leaders in charge and credit cards, Travelers Cheques, travel, network services and international banking.<sup>1</sup> I appreciate the opportunity to testify today about the steps American Express is taking to prevent its Cards from being used to purchase child pornography on the Internet.

As we all know, the Internet has been an engine for economic growth, enabling millions of small and large businesses to flourish. Much of that growth has been fueled by payment cards, which account for over 80% of all Internet purchases.<sup>2</sup> While the Internet offers great opportunity for legitimate businesses, it can also serve as a source of funding for an illegal and pernicious industry like child pornography. At American Express, we are focused on doing our part to block such funding.

My testimony today will describe American Express' business model, which differs in significant ways from the other major card networks. It will list the steps American Express has taken to ensure that its network is not used to process payments to purchase child pornography. Finally, it will outline what we are doing to focus even more intensely on combating this evil,

---

<sup>1</sup>American Express had total charge volume on our network of \$484.4 billion in 2005.

<sup>2</sup>2005/2006 Study of Consumer Payment Preferences by the American Bankers Association and Dove Consulting. Together with P2P Services, which are often directly tied to credit or debit cards, 89% of Internet purchases are facilitated through payment cards.

through enhancements in our own policies and through our involvement in the Financial Coalition Against Child Pornography.

**Background**

American Express operates what is often referred to as a “closed-loop” network. We issue charge and credit cards to our customers, and we have the direct relationship with millions of merchants who accept American Express Cards. We also operate a Global Network Services business, in which we partner with select financial institutions in the U.S. and abroad who issue payment cards on our network.

Our model can be distinguished from an open network arrangement, such as Visa or MasterCard, where the companies process transactions and serve as the connecting point between the issuing bank, which has a relationship with the cardholder, and the acquiring bank, which has a relationship with the merchant. At American Express, all these functions take place within one company: we issue cards to customers, operate the network, and manage the relationship with merchants who accept our Cards.

Consequently, our work to combat child pornography involves activities that might be undertaken by two or three different entities in the open network model. First, we are responsible for screening merchants who wish to accept American Express Cards, as an acquiring bank would do in the open network model. Second, we track activity on our network constantly to ensure that merchants are not violating our policies, as Visa and MasterCard do. Finally, we work with law enforcement to respond to any potential illegal activity on our network, whether that activity involves cardholders, merchants, or both.

In combating child pornography on the Internet, American Express follows a strategy that begins with a comprehensive review when we sign up a new merchant. It continues with



ongoing monitoring of merchant transactions and a constant search of the Internet to ensure that merchants on our network are not attempting to sell child pornography in violation of their contract with us. And it involves our active participation in the Financial Coalition Against Child Pornography, to ensure that we can coordinate effectively with law enforcement and others in the industry.

**Merchant Acquisition Due Diligence**

American Express either restricts or prohibits the signing of merchants that fall within sixteen general categories, including merchants in illegal or high risk industries. As part of our screening process, we first work to ensure that a merchant who wishes to accept American Express Cards is not linked to any illegal activities, including child pornography. In addition, since 2000 the Company also has prohibited the acceptance of American Express Cards for the purchase of pornographic content on the Internet more generally. As I will detail later, our efforts in fighting child pornography have taken place within the context of this broader policy.

When a merchant wants to begin accepting the American Express Card, we conduct a series of checks to ensure the merchant is not in violation of our policies. For instance, as part of our due diligence practices, we screen new merchants through a derogatory matching process to determine whether we have canceled the merchant in the past for any reason. This search occurs real-time as part of the application process. We use the MasterCard MATCH system to determine whether any other acquirer has canceled the merchant for any reason. We also check new merchants against the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) lists to ensure that we are not signing up merchants who may be subject to U.S. sanctions or who may be operating in a prohibited country.

We then perform further due diligence on a risk-assessed basis. We conduct a financial background check, and we specifically review a merchant's website if the application raises concerns. Merchants that we view as a higher risk or that require additional screening are routed to an internal contract review team for further investigation.

American Express maintains a uniform policy for access to our network, and we have the right to terminate a merchant at any time. This enables us to communicate our policies in a clear and consistent way to our merchants, and if we suspect they are violating our policies, to take immediate action.

#### **Ongoing Monitoring for Prohibited Industries**

In addition to a review at the time of application, we continue to monitor merchants for suspicious activity after they have been approved to process transactions on our network.

American Express continually monitors merchant submissions to identify changes in submission patterns, looking for suspicious activity or patterns that are not consistent with the merchant's identified industry. For instance, if a merchant had a long period of inactivity, followed by a sudden surge in charge volume, this could trigger a review. If a store began having a high number of submissions through remote (i.e., over the Internet) sales, after signing as a "brick and mortar" merchant, this also could trigger a review.

Through various monitoring processes and the direct relationships with merchants, American Express is able to identify and investigate any activity that differs in an important way from what would be customary or expected for a particular merchant or industry. In doing so, we compare things like a merchant's overall charge volume and average transaction size to the normal patterns in an industry. This helps us detect merchants involved in businesses that are different than those they identified at the time of their signing.

In the case of Internet merchants, American Express conducts ongoing monitoring of the worldwide web to detect illicit activity. Through a constant sweep of the web and a regular review by our own internal team, we search the Internet for websites that advertise acceptance of the American Express Card and operate in industries where we have prohibitions or restrictions on the use of our Cards.

American Express has contracted with an investigative firm that specializes in searching the web to detect any sites that may reveal a violation of our policies. This search employs web crawlers that are designed to imitate an individual, clicking on links to move deeper into a website, as well as those that do a more general review. These web crawlers review millions of web pages each day and specifically look for sites that contain objectionable content and that purport to accept the American Express Card. In the case of child pornography, this search includes proprietary technology to detect child pornography websites.

Following a search of the web, the results are combined and then scored using advanced algorithms to identify those sites most likely to be in violation of our policies. Our vendor then downloads sites that may be in violation of our policies and inspects them individually before sending a comprehensive report to our internal merchant risk operating team. This team then reviews the report and investigates further. Following this review, we cancel any merchant we identify that is in violation of our policies.

Our ongoing search of the web regularly discovers pornographic sites that mention American Express; a small number of those sites could have links to child pornography sites. In most cases, these websites include references to American Express but are not actually connected to one of our merchants and cannot process payments on our network. In these cases, we work to determine the operator of the website so that we can issue cease and desist notices that

demand the removal of any reference to American Express, which represents brand infringement. In instances where we identify an actual merchant violating our policies, we terminate the merchant.

As one example, last year we discovered twelve websites that appeared to be questionable child modeling sites based in South America, portraying pictures of children under the age of 18 in provocative clothing. These sites offered visitors the opportunity to purchase a subscription, but it did not appear that any of them accepted American Express Cards as a payment option. We have since referred these sites to NCMEC for further investigation to see if they might be linked to other child pornography sites reported to the Center.

By every indication, our policies and the steps we have taken to ensure compliance with those policies have prevented any extensive use of our network to finance child pornography. In cases where we have found a website that could be linked to child pornography, we have terminated the merchant. However, the vast majority of merchant cancellations in this area stem from violations of our broader policy banning the use of our Card for the purchase of Internet pornography.

The statistics from the National Center for Missing and Exploited Children are consistent with these findings. In 2005, a very small percentage of all commercial child pornography referrals received by NCMEC contained references to American Express. Our own experience indicates that very few of the sites that mention American Express are authorized to do so and actually connect to a merchant on our network.

For instance, this summer NCMEC provided us with twenty-four referrals that included references to American Express. Removing duplicate referrals of the same website, there were a total of nineteen unique sites, of which nine sites were no longer accessible. In reviewing the

remaining sites, another nine sites either did not link to a payment page or purported to accept our Card but did not in fact offer American Express as a payment option. After completing our investigation of these twenty four reports, we determined that only one site involved an American Express merchant. We immediately terminated that merchant and notified law enforcement as well as NCMEC.

While our research shows that very few child pornography sites take our Card, it appears that they often promote payment by credit cards to make the site appear more legitimate. It is extremely rare that a child pornography website will offer direct acceptance of credit card payments, but there is a growing trend toward steering visitors of these sites to various alternative payment methods. Operators of child pornography sites are developing increasingly complicated methods to collect payment, including the use of third-party payment providers to mask their activities.

While our restrictive rules have been broadly effective, we are focused on two areas where we can do more, and we have adjusted our policies and procedures accordingly. First, we have changed our process for monitoring the Internet. In the past our search for child pornography sites took place as part of our broader efforts to enforce our Internet pornography policy, and there was not always a clear differentiation between the two in our review and reporting. We now separately track and, if necessary, refer to law enforcement any sites that could include child pornography.

Second, through our work with the Financial Coalition Against Child Pornography, we have instituted a more effective, documented and ongoing consultation with law enforcement on child pornography issues.

**Financial Coalition Against Child Pornography**

American Express is proud to be a member with other financial services firms in the Financial Coalition against Child Pornography led by the National and International Centers for Missing and Exploited Children. We are pleased to join with others in the payments industry, Internet service providers, and law enforcement in this effort to end commercial child pornography. This cooperation between the public and private sector is a critical part of a comprehensive strategy to eradicate the evil of child pornography.

We believe one of the most important aspects of the coalition is the opportunity to deepen our collaboration with our peers in the industry, law enforcement, and experts at the National Center for Missing and Exploited Children. The Financial Coalition has established a formal process for reporting suspected child pornography websites, with the National Center for Missing and Exploited Children serving as a global clearinghouse. The work of the Center will also institutionalize the cooperation between law enforcement and financial services firms in this ongoing battle. This closer cooperation with law enforcement will have a very positive impact on our effectiveness and, I believe, the effectiveness of the industry as a whole in combating child pornography.

In closing, I want to applaud the members of this committee and your staff for drawing attention to this critical concern. American Express is committed to working in partnership with law enforcement and others in the industry to deny child pornographers access to the payment system, and we appreciate your focus on this important issue. Thank you for the opportunity to testify today, and I would be happy to answer any questions you may have.

MR. WHITFIELD. Thank you, Mr. Christenson. Ms. Golinsky, you are recognized for a 5-minute opening statement.

MS. GOLINSKY. Good afternoon, Chairman Whitfield and Ranking Member Stupak. My name is Jodi Golinsky, and I am Vice President, Regulatory and Public Policy Counsel at MasterCard Worldwide. It is my pleasure to appear before you today to discuss our efforts to prevent the misuse of our system in connection with online child pornography.

We commend the subcommittee for its leadership on this issue. The efforts of the subcommittee and its staff have increased the focus on this issue and have helped bring together a wide range of interests to combat child pornography.

MasterCard deplores any attempts to use our system for illegal purposes, and we are deeply committed to combating the sale of child pornography. Our efforts in this area include, one, working to prevent offending websites from accepting MasterCard-branded payment cards, two, detecting websites attempting to circumvent our prohibition, and, three, assisting law enforcement to detect, apprehend, and prosecute child pornographers. We have had great success in impeding these criminals from accessing our system. We recognize, however, that we see only part of the problem and that criminals who are denied access to our system are quick to look for other payment alternatives.

We also recognize that private sector efforts alone are simply not enough. Collaboration with law enforcement is critical. Law enforcement must be given the tools and resources to apprehend and prosecute these criminals, and there must be an effective mechanism for the private sector to assist law enforcement in achieving those objectives. To address these issues, MasterCard has partnered with the National Center for Missing and Exploited Children to form the Financial Coalition Against Child Pornography. In conjunction with government leaders and law enforcement agencies around the world, the coalition has embarked on a first of its kind globally focused effort to identify and eliminate commercial sources of child pornography.

I want to discuss more directly MasterCard's efforts to combat this problem as well. MasterCard has a series of rules that require financial institutions who contract with merchants, also known as acquiring banks to insure that the merchants are legitimate and engaged in solely legal activities. These rules mandate, among other things, that acquirers perform due diligence before authorizing merchants to accept MasterCard payment cards and that acquirers monitor merchants on an ongoing basis for compliance with the rules. We have also proactively educated our customer financial institutions around the world about our rules and their obligations with respect to illegal transactions such as child pornography.

MasterCard also works closely with law enforcement officials to assist them in detecting and prosecuting child pornographers. In addition, we undertake significant efforts to check child pornographers seeking to circumvent our controls. These efforts include searching the Internet to identify sites that appear to be selling child pornography and purporting to accept our cards as payment. In the overwhelming majority of cases where our brand appears on the site, we have found the

site does not actually accept our cards but impermissibly displays our logo.

Our success in impeding these criminals from using our system does not end the problem however. We have seen a clear trend in which child pornographers denied access to our system are moving rapidly toward alternative payment methods to avoid detection and prosecution. We are not, therefore, content to simply drive these criminals from our system and are devoting considerable resources to a more comprehensive approach to dealing with the problem. We believe that our partnership with NCMEC and the coalition provides such an approach.

MasterCard provides to NCMEC the fruits of our investigative efforts and other information that may be helpful to them. NCMEC in turn investigates and then refers this information to the appropriate law enforcement officials who are given the opportunity to conduct their own investigation. If law enforcement decides to proceed with an investigation, we work with law enforcement to support their efforts. If law enforcement decides not to proceed, a notice is sent to any payment service provided on that site and those services work to terminate payment acceptance at that site.

In addition to our active participation in the coalition, MasterCard is also a corporate sponsor NCMEC. MasterCard views our sponsorship of NCMEC as an extension of our fight against the exploitation of children and dissemination of child pornography on the Internet, and we are extremely proud to contribute to their efforts. Chairman Whitfield, Ranking Member Stupak, thank you again for the opportunity to discuss these important issues with you today. MasterCard is deeply committed to doing its part to eliminate the commercial viability of child pornography on the Internet. It has also been our pleasure to work with your staff, with NCMEC, with law enforcement and others to help develop solutions to this problem, and we look forward to continuing those efforts. I would be happy to answer any questions that you may have.

[The prepared statement of Jodi Golinsky, Esq. follows:]

PREPARED STATEMENT OF JODI GOLINSKY, ESQ., VICE PRESIDENT AND SENIOR  
REGULATORY COUNSEL, MASTERCARD INTERNATIONAL, INC.,

Good morning, Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee. My name is Jodi Golinsky, and I am Vice President, Regulatory and Public Policy Counsel at MasterCard Worldwide in Purchase, New York. It is my pleasure to appear before you today to discuss our efforts to prevent the misuse of our system in connection with on-line child pornography. We commend the Subcommittee for its leadership on this issue. The efforts of the Subcommittee and its staff have increased the focus on this issue and have been helpful in bringing together a wide range of interests to combat child pornography.



MasterCard deplores the use of our system for any illegal purposes, and we prohibit our system from being used for the sale of child pornography. We take this matter very seriously, and we are committed to combating the sale of child pornography. Our efforts in this area include: (i) working to prevent offending web sites from accepting MasterCard-branded payment cards; (ii) investigating and testing to detect web sites attempting to circumvent our prohibition; and (iii) assisting law enforcement to detect, apprehend, and prosecute purveyors of child pornography.

These efforts have succeeded in significantly disrupting child pornography sales. We recognize, however, that we see only part of the problem and that criminals who are denied access to our system are quick to look for other payment alternatives, including new and evolving payment methods designed for Internet-based transactions. We also recognize that private sector efforts alone are not enough—collaboration with law enforcement is critical. Law enforcement must be given the tools and resources to apprehend and prosecute these criminals, and there must be an effective mechanism for the private sector to assist law enforcement in achieving those objectives.

To address these issues, MasterCard has partnered with the National Center for Missing and Exploited Children (“NCMEC”) to form the Financial Coalition Against Child Pornography (“Coalition”). The Coalition represents a partnership of companies and governmental entities that have come together to combat child pornography. It includes a broad range of financial institutions, Internet service providers, and technology companies committed to working with NCMEC and governmental agencies to develop a coordinated approach to detecting and combating child pornography and provide a critical mechanism for assisting law enforcement in developing the information needed to apprehend and prosecute these criminals.

Coordinated by the NCMEC and the International Center for Missing and Exploited Children, the Coalition has embarked, in conjunction with government leaders and law enforcement agencies worldwide, on a first of its kind, globally focused effort to identify and eliminate commercial sources of child pornography. The Coalition has defined an initial four-point strategy to combat child pornography that stresses the sharing of information about illegal activities among Coalition companies and has created a centralized system that proactively seeks, reports, and tracks the dissemination of child pornography. This information sharing is designed to provide law enforcement the essential information they need to apprehend and prosecute the criminals that purvey child pornography. It also provides an efficient mechanism for the Coalition’s private sector participants to obtain the information needed to shut down the services being utilized by the criminals.

In addition, the Coalition is mobilizing world leaders to become a part of this global effort to eradicate child pornography. Through collaboration with this broad range of partners, we are mounting an aggressive effort against child pornography. Indeed, as discussed below, the Coalition has developed a mechanism to allow law enforcement and private sector parties to share valuable information to reduce the viability of child pornography web sites.

### **Background**

MasterCard is a global organization with 25,000 financial institution customers that are licensed to use the MasterCard service marks in connection with a variety of payments systems. It is important to note that MasterCard itself does not issue payment cards nor does it contract with merchants to accept those cards. Instead, those functions are performed by our customer financial institutions. The financial institutions that issue payment cards bearing the MasterCard brands are referred to as “card issuers.” The financial institutions that enter into contracts with merchants to accept MasterCard-branded cards are referred to as “acquirers.” MasterCard provides the networks through

which the customer financial institutions interact to complete payment transactions and sets the rules regarding those interactions.

#### **Efforts to Address Child Pornography**

A fundamental rule of our system is that each customer financial institution must conduct its MasterCard programs and activities in accordance with all applicable laws. This includes, for example, ensuring that any transaction a customer submits into the MasterCard system pertains to only legal activity. In connection with this rule, MasterCard expressly prohibits the use of its brand or system in connection with child pornography transactions, regardless of any legal ambiguity that may exist in a given jurisdiction.

MasterCard also has a series of rules that require acquirers to ensure that the merchants with whom they contract to accept MasterCard-branded cards are legitimate and engage in solely legal activities. These rules mandate, among other things, that acquirers perform due diligence on a merchant before authorizing the merchant to accept MasterCard payment cards and that acquirers monitor merchants for compliance with the rules. Acquirers that fail to comply with the rules may be required to absorb the cost of any illegal transactions, and may be assessed fines, suspended or terminated, in MasterCard's sole discretion.

It is important to note that we have been proactive in educating our customer financial institutions about our rules and their obligations with respect to illegal transactions, such as child pornography. For example, MasterCard has provided acquiring banks with guidance based on intelligence we have gained from previous investigations so acquirers are better prepared to avoid criminal or fraudulent schemes. In fact, we have also stressed the importance and utility of the Coalition to our customer financial institutions which has resulted in the recruitment of several Coalition participants.

MasterCard also works extensively with law enforcement officials to address situations where the legality of activities related to MasterCard payment card transactions is in question. A major objective of these efforts is to ensure that MasterCard provides appropriate support to law enforcement in their efforts to address illegal activity. We are sensitive to the fact that our efforts to enforce the MasterCard rules have the potential to hinder ongoing law enforcement investigations and the like. For example, when a merchant is shut off from accepting MasterCard-branded cards because the merchant violated our rules, law enforcement's ability to gather evidence can be impeded and shutting off a merchant might alert that merchant to an ongoing investigation.

In addition, MasterCard undertakes significant efforts to detect child pornographers seeking to circumvent our controls. These efforts include searching the Internet to identify sites that appear to be selling child pornography and purporting to accept our cards as payment. Once such sites have been identified, a painstaking, and largely manual, investigation is conducted to determine whether those sites actually accept our cards. In the overwhelming majority of cases where our brand appears on the site, we find that the site does not actually accept our cards but impermissibly displays our logo. Unfortunately, our success in impeding these criminals from using our system does not end the problem. We have seen a clear trend in which child pornographers denied access to our system are moving rapidly toward alternative payment methods to avoid detection and prosecution.

Consequently, we are not content to simply drive these criminals from our system and are deeply committed to a more comprehensive approach to dealing with the problem. We believe that our partnership with NCMEC and the Coalition provides such an approach, and we are in the process of conducting a program with the Coalition and law enforcement which is designed to make it more difficult for criminals driven from our system to find safe haven. Under the program, MasterCard is providing to NCMEC

the fruits of our investigative efforts. NCMEC, in return, refers this information to the appropriate law enforcement officials who are given the opportunity to conduct their own investigation. If law enforcement decides to proceed with an investigation, we work with law enforcement to support their efforts. If law enforcement decides not to proceed, a notice is provided to any payment service provided on that site and those services work to terminate payment acceptance at that site. This approach gives priority to any law enforcement efforts to investigate and prosecute the offending criminals but also helps to ensure that the criminals are thwarted from their efforts to receive payment when law enforcement is unable to pursue prosecution.

In addition to our active participation in the Coalition, MasterCard is also a corporate sponsor of NCMEC. MasterCard views its sponsorship of NCMEC as an extension of our commitment to helping fight the exploitation of children and dissemination of child pornography on the Internet, and we are proud to contribute to NCMEC's efforts.

### **Conclusion**

Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee, thank you again for the opportunity to discuss these important issues with you today. MasterCard is deeply committed to doing its part to eliminate the commercial viability of child pornography on the Internet. It has also been our pleasure to work with your staff, NCMEC, law enforcement, and others to develop solutions to combat child pornography. We look forward to continuing these efforts. I would be glad to answer any questions you may have.

MR. WHITFIELD. Thank you very much. And, Mr. Sullivan, you are recognized for 5 minutes.

MR. SULLIVAN. Thank you, Chairman Whitfield, and Ranking Member Stupak. My name is Joe Sullivan, and I am the Associate General Counsel at PayPal. I am grateful for the opportunity to speak with you today about the steps that PayPal has been taking to combat the financing of child exploitation on the Internet. Both the efforts we have taken on our own, and the progress we have made working together with the other members of the Financial Coalition. I am very familiar with PayPal's efforts in this area. I spent my first 4 years at the company overseeing our work with law enforcement, and I have personally engaged the FBI, ICE, Scotland Yard, and other agencies on this important issue.

I am also very familiar with the challenges of tracking online predators because I have personally prosecuted Internet child exploitation cases while working for the Department of Justice, first as the high tech prosecutor at the U.S. Attorney's Office in Las Vegas, and later as a founding member of the first full-time high tech Federal prosecution unit at the U.S. Attorney's Office in the northern district of California. I am very grateful I had the opportunity to work under current FBI Director Robert Muller when he was the U.S. Attorney when he made the smart decision to found and create the first high tech dedicated unit.

PayPal is the global leader in online payments, and is a wholly owned subsidiary of eBay. The way PayPal works is to enable individuals and businesses to pay and accept payments securely on the Internet. We are built on the existing financial infrastructure of banks and credit cards. We have more than 114 million accounts around the world. PayPal is committed to providing a safe and legal online payment service for its users. We are very clear with our customers about the types of transactions that we do allow and don't allow, and certainly the use of PayPal for the purposes of sending or receiving payment for child pornography is strictly forbidden.

It is clearly in our interest and that of the public that we know who our customers are, how they transact online, and whether the intent to comply with our acceptable use policies. A safe well-lit Internet serves all constituents as well, and to that end we dedicate significant resources to our efforts. In particular, we focus on three areas, technology, partnerships, and coordination with law enforcement. At its heart, PayPal is a technology company. It is made up of engineers, statisticians, and scientists, and we use very sophisticated behavioral and anti-fraud models which literally get smarter with every transaction that goes through our systems. We have patented unique and sophisticated anti-fraud techniques and our approaches are emulated across the Internet.

We view our technology as a strong front door. We use modeling to screen registrations, evaluate user associations, scrutinize transaction details, and detect suspicious patterns. On the topic of modeling, we have developed over time a sophisticated lexicon of key words to use in child pornography related searches, and we have done so with the help of law enforcement agencies such as the FBI's Innocent Images Group and Scotland Yard, which have contributed significantly to refining our key word lists. We also proactively searched the Internet using search engines and Web scraping services and we hire external experts to supplement our efforts. Collectively, we review hundreds of thousands of URLs and business models each year.

As part of the united front, we work closely with our partners at the National Center, the credit card associations, financial institutions, Internet service providers, and other technology companies. We are all in this together and we work together well to leverage our combined expertise and develop best practices to deter the exploitation of children online. We were excited to be founding members of the Financial Coalition and even more excited about the progress the group had made to date. The passion of Ernie Allen and his team at the National Center combined with the expertise of the financial industry and the commitments of law enforcement make a powerful combination.

We also work proactively with law enforcement. We don't wait to be called. When we find anything remotely linked to the distribution of child pornography, we do three things. We send a report to the National Center. We file a suspicious activity report, and we package the details up in a proactive referral to law enforcement. We also actively sponsor law enforcement Internet crime training conferences and we speak regularly at their training programs. From FLETCE to Quantico to the DOJ National Advocacy Center to the annual ICAC conference in San Jose our team of experts is always invited and always welcome.

These efforts together have certainly aided in the deterrence of child exploitation on the Internet but we are not content to stand still. We will continue to improve our technology and broaden and deepen our partnerships. We applaud the efforts of the committee to facilitate dialogue in further coordination. We believe that there are additional avenues that would further this objective such as pushing for Whois standards that will help with transparency for all commercial actors online, encouraging hosting services to have the ability to respond to third party requests without risk of liability, and enhancing dedicated law enforcement funding in this area.

These steps combined with the ongoing efforts of law enforcement will go a long way towards eliminating this horrible crime. Mr. Chairman, Mr. Stupak, thank you for your time, and I am happy to answer any questions.

[The prepared statement of Joe Sullivan, Esq. follows:]

PREPARED STATEMENT OF JOE SULLIVAN, ESQ., ASSOCIATE GENERAL COUNSEL, PAYPAL,  
INC.

Thank you Chairman Whitfield, Ranking Member Stupak, and members of the Committee. I appreciate the chance to talk to you today about the steps that PayPal takes to combat the financing of child exploitation on the Internet. We commend the Committee on its attention to this issue.

My name is Joe Sullivan and I am the Associate General Counsel for PayPal, Inc. Prior to joining PayPal, I served as Associate General Counsel for eBay, with responsibility for overseeing company relations with law enforcement and regulatory agencies in the United States and Canada, directing the company's Fraud Investigations Team and determining legal policies related to listing of items on eBay. Prior to joining eBay, I spent eight years working as an attorney for the United States Department of Justice. Most recently, I served as an Assistant United States Attorney in the San Jose Branch Office of the United States Attorney's Office for the Northern District of California. I was a founding member of the Computer Hacking and Intellectual Property Unit, based in Silicon Valley. Before joining that office, I practiced at the United States Attorney's Office for the District of Nevada, Las Vegas branch, overseeing the investigation and prosecution of high-technology crimes in that district, including the prosecution of child pornography cases.

As you know, PayPal is a financial service that allows individuals and businesses to pay and accept payment securely on the Internet. PayPal is built on the existing financial infrastructure of banks and credit cards, and has more than 100 million accounts around the world.

PayPal is committed to providing a safe and legal online payment service for its users. We have been very clear with our customers about the types of transactions that are allowed on our service. And certainly, the use of PayPal for the purposes of sending or receiving payment for child pornography is strictly forbidden.

It is clearly in our interest and that of the public that we know who our customers are, how they transact online, and that they are compliant with the policies set forth by PayPal. A safe, well lit environment serves all constituencies well and to

that end, we have 5000 employees dedicated to building our systems and upholding our policies.

Because of the horrendous nature of this crime, we rigorously enforce compliance with this prohibition. To combat the exploitation of children online, PayPal has dedicated significant resources in three areas: technology, partnerships, and coordination with law enforcement.

- PayPal is recognized as a leader in fraud and abuse prevention, and we view technology as a strong front door in protecting our customers. We use very sophisticated behavioral and anti-fraud models, which literally get smarter with every transaction that goes through our system. We also compare account information to internal and external databases as part of our effort to continually evaluate the risk profile of our customers. We use specialized technology to search the Internet for suspicious websites and we also pay third party services to help us detect illegal activity online.
- As part of a united front, we work closely with our partners at NCMEC, the card associations, financial institutions, Internet Service Providers, and the Financial Coalition Against Child Pornography. We work together to leverage combined expertise, and to develop best practices to deter the exploitation of children online.
- We also work extensively with law enforcement. We have a dedicated team of specially trained employees that works closely with law enforcement authorities on child pornography and other related cases. We train law enforcement annually. We also alert law enforcement when we spot suspicious activity, and we support their investigations and processes all the way through to the successful conviction of offenders.

These efforts have certainly aided in the deterrence of child exploitation on the Internet. But we are not content to maintain the status quo: we will continue to improve our technology, and deepen and broaden our partnerships to combat this crime.

We applaud the efforts of the Committee to facilitate dialogue and additional coordination among all members of our community to combat the exploitation of children online. We believe that there are additional avenues that would further this objective, such as providing law enforcement with additional resources, promoting better data retention policies, and improving the accuracy and usefulness of Whois data that identifies domain name registrants. These three steps would further advance the efforts of financial institutions like PayPal, as well as law enforcement, as we continue to fight this horrendous crime.

Mr. Chairman, members of the Committee, thank you again for inviting me to testify today. I would be happy to answer any questions.

MR. WHITFIELD. Thank you, Mr. Sullivan. Mr. McCarthy you are recognized for 5 minutes.

MR. MCCARTHY. Chairman Whitfield and Ranking Member Stupak, my name is Mark McCarthy. I am Senior Vice President for Public Policy for Visa. Thanks for the opportunity to testify today at this hearing. Mr. Chairman, Visa does not allow its payment system to be

used for any illegal activity, including child pornography. The crime of child pornography is such a heinous exploitation of the vulnerable and the innocent that we have decided to put in place since 2002 a program to search the Internet to find child pornography merchants and to expel them from our system. I want to describe that program for you today but first I want to start with the Coalition Against Child Pornography which Ernie Allen talked to you about in the earlier panel.

Visa cannot conduct a successful campaign against child porn alone. We need to share information. We need to work collaboratively with others. That is why, Mr. Chairman, as you heard in the previous panel, Visa and other payment systems have joined with the National Center for Missing and Exploited Children to form the Financial Coalition Against Child Pornography. This effort reflects our shared belief that child pornography is a global problem in need of a coordinated response. Together with our coalition partners, we will enhance our efforts to identify websites and pinpoint merchants that are trafficking in this illegal activity. We will cut them off from the use of our networks and we will provide assistance as we have in the past to law enforcement to put them in jail for good.

Our zero tolerance anti-child pornography program has two parts. The first, as I said, is due diligence requirements to prevent merchants of this character from entering our system to begin with. The second is the monitoring program to detect and expel any child pornography merchants that fraudulently gain access to our system. A quick word of background on our system. Visa itself performs the communication and settlement functions for our financial institutions. It is these financial institutions called acquirers that have the direct relationships with the merchants. And our rules oblige these acquirers to assume responsibility for their relationships with merchants.

A fundamental Visa rule is that they allow only legal transactions be submitted into the payment system. On child pornography, Mr. Chairman, our rules are explicit and clear, acquirers must insure that Internet merchants do not submit child pornography transactions into the Visa system, and they must terminate Visa acceptance immediately at any child pornography site that accepts Visa cards. You will hear more about what our acquiring financial institutions do in this area on the next panel. In general, they must determine that a prospective merchant is financially responsible and will abide by Visa requirements as well as by applicable law. By taking these precautions acquirers can and do provide a line of defense against child pornography merchants getting into our systems but these due diligence requirements are not a panacea.

Child pornography merchants do not present themselves as such to acquiring banks. They often appear to be legitimate merchants. They



use a variety of techniques to fool acquirers and thereby gain access to our system despite the best efforts of our acquiring banks to keep them out. Accordingly, Visa has a monitoring system to identify and eliminate child porn transactions. Since 2002 Visa has retained the services of an outside firm to search the Internet for child pornography and to find those sites that are child pornography sites and that are also accepting Visa cards.

Our search program was designed to identify and expel from our system exactly the kind of commercial porn schemes that you might have heard about in the past discussion of this issue. Mr. Chairman, our search firm uses advanced Web crawling and filtering technology to detect child porn websites. It looks for websites that display the Visa logo and that satisfy one or more indicators that they are engaged in the sale of child pornography or that they are marketing themselves as engaged in child pornography. These sweeps are ongoing. They are conducted 24 hours a day, 7 days a week, 365 days a year. Hundreds of millions of Web pages are searched each month.

When our search firm finds one of these criminal sites, they conduct test transactions to see whether in fact the site is accepting Visa cards or whether it is merely purporting to accept Visa cards. The search firm tells us immediately if they find a child porn site that is accepting Visa cards and unless requested by law enforcement to leave the site open Visa tells the acquiring bank to stop processing these transactions immediately. If these identified sites are not in fact accepting Visa cards but they are merely using the trademark Visa uses its best efforts to find the Web hosting company that is involved to direct them to remove the Visa logo.

We provide this information to NCMEC, to U.S. and international law enforcement agencies as well. Mr. Chairman, Visa's anti-child pornography program has made progress since we started the program in 2002. Our recent numbers tell the story. In August of this year our search firm examined over 11 million Internet sites a day and found two child pornography sites that accepted Visa cards. Of course, that is two too many. Since the beginning of this year nine such sites have been identified. All of these sites were quickly expelled from the Visa system.

In conclusion, Mr. Chairman, let me repeat the point that I began with. The way forward lies in collective action. Visa intends to continue and to increase our cooperative efforts with law enforcement and with the Financial Coalition Against Child Pornography. Mr. Chairman, I would be happy to answer any questions you might have.

[The prepared statement of Mark McCarthy follows:]

PREPARED STATEMENT OF MARK MCCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY,  
VISA U.S.A., INC.

Chairman Whitfield, Ranking Member Stupak and Members of the Subcommittee, my name is Mark MacCarthy. I am the Senior Vice President for Public Policy for Visa U.S.A. Inc. Thank you for the invitation to participate in this hearing. Visa appreciates this opportunity to testify as part of the Committee's investigation into the exploitation of children on the Internet.

The Visa Payment System is one of the leading consumer payment systems in the world. Visa itself performs communication and settlement services for participating financial institutions. The financial institutions that participate in the Visa system are the entities that issue Visa payment cards to individual consumers and authorize merchants to accept Visa payment cards in payment for transactions. Visa itself does not have direct relationships with merchants that accept Visa payment cards. In the jargon of the industry, the financial institutions that have a direct relationship with the merchants that accept Visa payment cards are called acquiring financial institutions or acquirers.

Visa rules require acquiring financial institutions to assume responsibility for their relationships with merchants. A fundamental Visa rule is that these acquirers submit only legal transactions into the Visa payment system. In addition, Visa has an explicit rule obligating acquirers to ensure that Internet merchants do not submit child pornography transactions into the Visa system.

Visa recognizes that payment cards are an important part of electronic commerce and believe that we have responded, and continue to respond, effectively to the challenges posed by Internet transactions. In addition to our rule against introducing illegal transactions into the Visa payment system and our explicit rule against child pornography transactions, Visa has a long history of working with law enforcement where the Visa Payment System may have been used in connection with illegal transactions. In this regard, Visa maintains ongoing working relationships with a variety of law enforcement agencies including the Secret Service, the Federal Bureau of Investigation, the Federal Trade Commission, and state and local law enforcement.

Our anti-pornography program has two components. The first is a set of due diligence requirements designed to prevent child pornography merchants from entering our payment system. The second is a monitoring program to detect and expel from our system any child pornography merchants that manage to fraudulently enter our system despite the best efforts of our acquiring banks to keep them out.

But first I want to mention our involvement with the Financial Coalition Against Child Pornography. Visa has made substantial progress with its own anti-child pornography program. So have the other major payment systems. But we cannot do it alone. We need to share information and work collaboratively together. That is why under the leadership of Senator Shelby, Visa, other payment systems and financial institutions joined with the National and International Centers for Missing and Exploited Children to form the Financial Coalition Against Child Pornography. In March of this year, there was a public launch of this program at a press conference with Senator Richard Shelby. This effort reflects our shared belief that child pornography is a global problem in need of a coordinated response. For many years, Visa has worked on its own to rid our system of this deplorable activity. By joining the Coalition, we reaffirmed and strengthened our long-standing commitment to doing our part to prevent the exploitation of children. Together with our Coalition partners, we will enhance our efforts to identify Web sites and pinpoint merchants that are trafficking in this illicit activity, cut them off from use of our networks, and provide assistance to law enforcement to shut them down for good.

### Visa's Due Diligence Requirements

Visa requires acquiring financial institutions to ensure that all merchants are properly qualified to accept Visa cards. Visa acquirers must determine that a prospective merchant is financially responsible, and will abide by Visa requirements, as well as applicable law. There are a variety of methods that acquirers may use to determine these qualifications, including credit reports, business financial statements, and income tax returns, conducting physical inspections of the business premises of a prospective brick and mortar merchant, and for electronic commerce merchants obtaining a detailed business description and examining the merchant's Web site.

By taking these precautions, acquirers can provide a line of defense against child pornography merchants entering the Visa system. These due diligence requirements are closely observed by acquirers, but they are not a panacea for addressing the problem of the use of Visa cards for child pornography transactions. Child pornography merchants do not present themselves as such to acquiring financial institutions. They often appear to be legitimate merchants. They use a variety of techniques to fool acquirers and thereby gain access to the Visa system, despite the best efforts of these acquirers to screen them out of the system.

### Anti-Child Pornography Program

Accordingly, Visa has supplemented these due diligence requirements with an explicit program directed against child pornography transactions. The elements of this program are

- An explicit rule prohibiting any Visa financial institution from acquiring these transactions
- A series of specific penalties for violation of this policy
- A program of searching the Internet to detect any website that appeared to be accepting Visa cards for child pornography transactions and processes to immediately stop this acceptance

An explicit ban against child pornography transactions within the Visa system is the first part of this program. Acquiring financial institutions are under an obligation to carefully review the website names and URLs of their Internet merchants to ensure these prohibited merchants are not operating within their portfolios. Acquiring financial institutions must ensure that all prohibited activity is immediately halted.

Violation of this policy may subject the offending acquirer to significant penalties including the imposition of conditions and termination of Visa Membership privileges. Visa acquiring financial institutions have been notified and reminded of these penalties several times since 2002. If Visa identifies a child pornography merchant in their portfolio, they must terminate the merchant immediately. If the merchant is not terminated within 7 calendar days, the bank is fined. Repeated offenses are punished with a system of escalating fines and other sanctions including preventing the offending acquiring financial institutions from signing up any new Internet merchants, requiring them to terminate existing Internet merchants and ultimately revocation of their Visa acquiring license.

Visa has not found it necessary to use these sanctions often. Early in our program some acquiring banks were initially reluctant to follow these required procedures. They were fined. They got the message. Since then, Visa acquirers have abided by our policy against child pornography.

In support of our efforts to keep child pornography transactions out of the system, Visa maintains a monitoring campaign to identify and eliminate transactions emanating from child pornography merchants. Since 2002, Visa has retained the services of an outside firm to search the Internet for child pornography websites that appear to be accepting Visa payment cards. This firm uses advanced web crawling and filtering

technology to detect these websites. It looks for websites that display the Visa logo, and that satisfy one or more indicators that they are engaged in the sale of child pornography or are marketing themselves as engaged in that business. The sweeps are ongoing; they are conducted daily and search hundreds of millions of web pages each month.

When our search firm detects one of these problematic sites, they conduct test transactions to see whether in fact the site is accepting Visa cards or whether they are merely illegally using our trademark on their site. The search firm tells us immediately if they find a site that is accepting Visa cards for these transactions. Unless requested by law enforcement to leave these sites open, Visa then contacts any acquirer found to be processing these child pornography transactions and directs them to stop processing these transactions immediately. If they have not done so within 7 calendar days, they are fined. If these identified sites are not in fact accepting Visa cards, but are merely using the Visa trademark on their site, Visa uses its best efforts to locate the web hosting company to direct them to remove the Visa logo.

In addition, Visa provides information regarding all these sites to U.S. and international law enforcement officials and to the National Center for Missing and Exploited Children. At their request and as part of an ongoing law enforcement investigation, Visa would allow these problematic sites to remain operational.

Visa's anti-child pornography program is making significant progress in the fight against the use of our payment system for these activities. Our experience is that fewer child pornography sites are displaying the Visa logo now than when we started the program in 2002 and that alternative payment mechanisms are increasingly the way these transactions are financed.

The way forward lies in collective action. We need to share information and work collaboratively together with other payment system providers and with law enforcement. Visa has recently taken an additional cooperative step in its anti-child pornography efforts. In April 2006 Visa signed a three-year partnership agreement with the newly created Child Exploitation and Online Protection Centre (CEOP), a London-based law enforcement agency. CEOP carries out proactive investigations worldwide and provides a single point of contact for the public, law enforcers and the communications industry, enabling suspicious activity to be reported direct, 24 hours a day. The unit, staffed by about 100 police, computer technicians and child welfare specialists, also offers advice to parents and potential victims. As a CEOP partner, Visa will provide not only financial support, but also use our knowledge and resources to strengthen the Center's Finance Desk. This uses financial investigation tools to identify people engaged in the sexual exploitation of children for profit, setting out to confiscate offenders' assets and disrupt their activities.

In addition to this work with CEOP, Visa intends to continue and to increase our cooperative efforts with law enforcement and with other payment systems in the Financial Coalition Against Child Pornography.

Visa appreciates the opportunity to appear before you today. I would be happy to answer any questions that you may have.

MR. WHITFIELD. Thank you, Mr. McCarthy. Dr. Jackson, you are recognized for 5 minutes.

MR. JACKSON. Mr. Chairman, members of the subcommittee, thank you for the opportunity to participate in these hearings, and, frankly, to respond to the concerns that have been raised regarding e-gold, my company. I am Douglas Jackson, the founder and Chairman of e-gold. I am also the CEO of Gold and Silver Reserve, which operates the OmniPay service. My background is that I am a physician, Board-

certified in radiation oncology. I have lived in Melbourne, Florida for the past 14 years. I have been married for 28 years. I have two children, boys aged 10 and 15. I conceived of e-gold 10 years ago, and deployed it online in 1996 as institution to advance the material welfare of mankind bringing access to global markets with reliable, efficient payment capabilities.

The business case for e-gold is introduced in my submitted testimony. This morning and in the media, I have heard the chant anonymous, untraceable, and inaccessible to law enforcement applied to my company. I am here to tell you that that is simply nonsense. The inaccessible to law enforcement bit, we have been reaching out proactively to law enforcement since 1999. Recently, fortunately, we get some response. Recently, the cooperative arrangements have improved. We owe a great debt to Ernie Allen of NCMEC for that relationship which in this area of child pornography led to a C change. Instead of agencies keeping sites secret from us on some strange presumption of complicity, instead bringing them to our attention and getting the initial tools that we needed to develop the protocols for detection and interdiction.

As far as anonymous and untraceable, it is simply not the case. E-gold is a book entry mechanism. If a criminal uses e-gold for a transaction it is the career ending, game over mistake, and our transactions are permanent. I see my red light is on. I want to direct your attention to page 13--

MR. WHITFIELD. You still have two minutes and 59 seconds. We forgot to reset it.

MR. JACKSON. Okay. I don't know how to do that. Sorry. Page 13 of the submitted testimony has a graph. It tells our whole story. It shows the success story over the past year where we have had a 98 percent reduction in the amount of child pornography payments that are processed through the e-gold system. If there is the slightest skepticism regarding these numbers, I encourage you to appoint one of your staffers, one that is technically savvy, detail them for 2 days, have them spend time with our investigators, and we will satisfy them that this is the absolute case.

The remaining amount of this crime that is conducted through e-gold is meager. It is paltry. The declining trend will continue until we have it suppressed down to zero. I welcome any questions.

[The prepared statement of Douglas Jackson follows:]

PREPARED STATEMENT OF DOUGLAS JACKSON, CHAIRMAN, E-GOLD GROUP, INC.

Mr. Chairman, members of the Committee on Energy and Commerce Subcommittee on Oversight and Investigations: thank you for the opportunity to participate in these

hearings. The problem of child pornography on the Internet is a serious one, and I am pleased to see the full involvement of the federal government, nongovernment organizations, and private industry. Working cooperatively will certainly help us all in the goal to eradicate this heinous crime from the Internet.

I would also like to applaud Ernie Allen and the National Center for Missing & Exploited Children (NCMEC) who have spearheaded the effort to bring together this financial coalition. Our aim, along with the NCMEC, is to curb the flow of payments to these criminals and to help identify perpetrators and their activity so that law enforcement can take appropriate action. We strongly support the NCMEC's goal to eradicate child pornography on the Internet, and I would like to add my thanks to my colleagues in this coalition.

I would like to take the opportunity to introduce you to e-gold. Though e-gold is approaching its tenth anniversary in November of this year, we recognize that we are still not well known in circles that do not make extensive use of the Internet for commerce. e-gold, Ltd. is a Nevis, West Indies company. It is operated by Gold & Silver Reserve (G&SR), headquartered in Melbourne, Florida. Gold & Silver Reserve also operates a service for the purpose of buying or selling e-gold, branded as OmniPay. Gold & Silver Reserve's primary mission is to establish e-gold as a viable and credible medium/mechanism for Internet payment transactions, allowing an easy, safe, and secure means to receive payment via the Internet.

#### **Overview**

e-gold® is a unique alternative system that mobilizes the value of gold for Internet payments. e-gold is designed to provide a complementary payment system for secure and final Internet transactions that minimizes exchange risk. Following charge cards, e-gold has the world's second largest reach as an online payment system behind PayPal, and it is far more global. Comparative analysis by websites that measure Internet activity show PayPal and e-gold first and second respectively in web traffic on payment system sites.

e-gold differs from every other existing payment system in that a quantity of e-gold constitutes a liability that, by virtue of a 100% reserve of physical gold, perfectly embodies the value of gold in allocated storage. e-gold is denominated in weight units. Transfers from account to account occur by book entry on dedicated database servers. E-gold is a closed system; that is, it is impossible for a user to send value into the system. Increases or decreases of the overall quantity of e-gold in circulation can be effected by bailment or redemption of physical gold by a credentialed entity, either a gold bank or other primary dealer designated by the issuer, e-gold, Ltd.

e-gold has over 3 million accounts in more than 165 countries and has the credibility of significant tenure, having been in operation online for almost 10 years. During e-gold's 10-year history, numerous other payment mechanisms have attempted to penetrate the online payment and remittance market, spending hundreds of millions to do so. PayPal, clearly the market leader, burned through \$275 million of losses before their acquisition by eBay. e-gold established its position almost entirely through the personal investment of its founder and a close circle of family and friends and has carefully continued its progress, relying on internally generated funds. e-gold has survived and thrived where most others have failed, due to a sound and coherent business model and robust, evolving self-governance as described below. This financing approach has not allowed the speed of growth that, for example, PayPal has achieved, but it has allowed e-gold to stay firm to its original mission. Classical market analysis would show organizations such as PayPal, Western Union, and credit card companies as competitors. In actuality, however, every seeming competitor would benefit from a strategic embrace of e-gold, taking advantage of e-gold's inherently global reach and non-repudiable settlement protocol to extend their own market penetration, reduce direct costs, and thereby offer a better service to their customer base. These same efficiencies, combined

with e-gold's ever more refined capabilities for detection and interdiction of illicit payment transactions, would provide substantial benefit to official institutions that accept payment online and/or which themselves offer remittance and related services, like the U.S. Postal Service,.

Since its inception, e-gold has settled over 67 million individual transactions and is today processing 50,000–70,000 account-to-account transfers per day, valued at over \$2.0 billion USD annually.

All e-gold in circulation is backed 100% by a reserve of physical gold in London Bullion Market Association member repositories. Currently, reserves amount to nearly 3.6 million Fine Grams of gold, which would place e-gold 76th among countries for the value of gold reserves. At today's gold exchange rates, this reserve is valued at over \$68 million USD.

### **Vision**

e-gold was established in 1995 as a viable and credible medium/mechanism for Internet payment transactions, allowing an easy, safe, and secure means to make account-to-account transfers of value on the Internet by anyone, anywhere in the world.

e-gold's governance and transaction model derives from the dual imperative to assure finality of settlement and freedom from default risk.

e-gold is a payment system that, unlike any other, allows people from any region or economic background to operate globally: a migrant worker can send value back home easily and a merchant can accept payment from someone in a third-world country who may be without access to a charge card or bank account.

e-gold alone is free of chargeback risk, yet the fees for receiving payment in e-gold are a tiny fraction of those charged by any other systems.

Thanks to e-gold, for the first time in history, normal people of modest means worldwide have the option of using a medium of exchange and store of value that is designed from the ground up to be immune to debasement with a governance model that precludes even its management and founders from having the power to subvert it.

### **Governance, Security, and Visibility**

e-gold has a firm governance model to protect its users, is highly secure, and offers unprecedented visibility of activity to its users.

e-gold remains independent of its Operator and any "exchangers" of e-gold, a separation of roles that further aids in assuring e-gold's freedom from default risk and finality of settlement. The operating guidelines are governed by the e-gold Account User Agreement which can be found on the e-gold website. The physical gold, stored in London Bullion Market Association recognized depositories in allocated storage, is titled to the "e-gold Bullion Reserve Special Purpose Trust," a purpose trust holding these physical assets for the exclusive benefit of e-gold account holders. The gold is not under the control of the owners or operators of e-gold.

Transfers within e-gold are account-to-account, with immediate settlement by book entry on dedicated servers.

e-gold payments are made in a weight-based unit of (typically) gold. This medium of payment makes e-gold less subject to extreme fluctuations in currency exchange rates, especially for customers in countries with unstable currency. The asset portfolio backing e-gold, consisting entirely of physical gold, is free from the financial risks that pertain to securities or other debt instruments.

Freedom from default and finality of settlement are essential features that set e-gold apart from other payment systems and have led to e-gold's firm position in the market. For e-gold to continue to grow and achieve its original vision, it is imperative that it maintain its low-risk model and operate at the highest level of integrity.

The e-gold system is very secure. All transactions occur online. Account login requires an account number, a pass phrase, human recognition of a Turing number, and a system verification of the user's IP address. The only instances e-gold has encountered with compromised accounts are those in which a user in some manner surrendered both their account data and access to their personal email to an unknown party. e-gold maintains significant information on its website to educate users to the various schemes used to gain account information.

e-gold abides by an unparalleled standard of transparency. The "Statistics" and "Examiner" links on the e-gold website publish real-time data on payment volume and other system usage data as well as the detailed inventory data for each repository. This transparency is unique among all online payment systems, including other precious metal-backed sites. We believe it is of fundamental importance that our customers fully understand e-gold's size, growth, and gold backing to establish the credibility for safe, ongoing use.

Very favorable critiques have been received from respected business journals. Both *Barron's* in April 2001 and *Grant's Interest Rate Observer* in June 2003 reported favorably on the e-gold system. *Barron's* noted: "The ideal e-currency might even be backed by gold. Encrypted digital units of the precious metal could in principle be used to pay for anything.....One company, E-gold already allows on-line users to settle payments using its currency, which is 100% backed by gold."

#### **e-gold's Commercial Advantages**

e-gold offers numerous advantages to both online merchants (recipients of payment) and to online consumers (payers). (With e-gold, this traditional merchant/consumer distinction is obsolete—e-gold is bi-directional, meaning every account can make or receive payments.) Merchants benefit from fees that are significantly lower than any other online payment system. All payments are immediate and final: there are no chargebacks and the possibility of fraudulent payments is eliminated. e-gold is the most global of all payment systems, with easy-to-use interfaces, including a shopping cart. Since e-gold itself is immune to credit-related risks such as default by a user, recipients of e-gold payments are free of the costs and risks that other systems are forced to pass to their payment recipients.

Consumers do not need to share personal information across the Internet to make a payment. This feature is a great advantage in reducing identity theft. Payment is immediate, final, and fully automated, enabling the purchased product or service to reach the consumer faster. Low transaction fees, coupled with elimination of costs associated with chargebacks can provide merchants a competitive edge by enabling cost savings to be passed back to the buyers. All transactions are fully traceable: if a debate ensues about a sale, there is a clear and unimpeachable record of the payment. And importantly, the e-gold payment system is easy to use.

#### **e-gold "Exchange"**

e-gold does not accept "money" (or any other transfer of value from the public) directly into the system. The only way to obtain e-gold is from someone who already has it. Many users will buy and sell their e-gold through a third-party "exchanger." These are organizations completely independent of e-gold that operate around the world. The "exchangers" will accept payment for e-gold in a number of ways, but most typically accept wire transfers or certified checks. Any entity performing exchange realizes a business necessity to "know their customer" in order to avoid fraud losses due to failed or reversed payments transmitted via legacy (conventional credit-based/bank mediated) mechanisms.

Gold & Silver Reserve's OmniPay serves as an exchanger and is the primary source of e-gold, buying from or selling to other exchangers as the market requires. OmniPay



has implemented significant controls on how and to whom they buy or sell e-gold. When a new user profile is created, it requires e-mail validation followed by confirmation of the postal address. The user is also required to prove control of any e-gold account to or from which the user intends to transact with OmniPay. User profiles are screened against OFAC and similar lists upon creation and with each exchange transaction that exceeds a threshold.

OmniPay will only sell e-gold upon confirmed receipt of a bank wire, further guaranteeing “know your customer” considerations. Upon selling e-gold, OmniPay will transmit by bank wire or a check delivered to the validated postal address.

All bank wires are reviewed to assure the transmitter name matches the name of the OmniPay user that entered the “exchange” order, and a permanent file of wire notifications is maintained. OmniPay restricts daily exchange from one party to \$100,000. If a larger amount is necessary, OmniPay requires significantly more due diligence, including notarized residence documents and copies of a government-issued photo ID. Inbound wire transfers are reviewed to ensure that the sending bank is not proscribed by U.S. Treasury guidelines.

#### **e-gold is Not Hospitable to Illicit or Criminal Activity**

All online payment systems are subject to the attempts of individuals to use them inappropriately, whether for acceptance of illegal funds, money laundering, or other illicit activity. e-gold’s unique features and investigative protocols make it the poorest choice a criminal could make.

Two fundamental elements coupled with numerous programmatic processes and controls eliminate the possibility of e-gold serving as a source of indirection or successful obfuscation of money trails.

1. The public is incapable of sending “money” into the system. e-gold, Ltd. has no bank accounts and no capability of accepting payment or holding value in the form of any national currency. Value can be added (via the bailment of good delivery bars into the Trust) only by an entity that has been fully vetted by one of the gold banks that comprise membership of the LBMA. Currently, only G&SR is credentialed to bail additional precious metal reserves into the system. A normal account user can obtain a quantity of the circulating medium (e-metal) only by receiving it in payment from another account user who already has some.
2. Value in the system is fully traceable. Transfers are executed by book entry, creating a permanent record of the lineage of every particle of value within the system. Records are maintained perpetually: the details of any transfer since the beginning of e-gold are available.

One of duties of the e-gold Operator (G&SR) is to conduct investigations pursuant to lawfully executed subpoenas or court orders. The organization of e-gold as a closed system where all transfers settle by book entry and all transactions capture supplemental information of potential forensic value eliminates the possibilities of a miscreant successfully using the system in an anonymous or untraceable fashion, even if false contact information has been provided. Upon its creation, an e-gold account contains no value and can only be “funded” by receiving payment from another user, thereby linking the newly funded account to a web of counterparties, some of whom inevitably will have provided correct and discoverable contact information. There has never been an investigation (over 75 performed per year) where the e-gold investigative staff has failed to identify the true identity of a suspect.

A new user may create an account online. The prospective user is required to provide contact information, including name, e-mail address, postal address, and telephone number. To validate the e-mail address, the system sends a welcome message

to the specified e-mail address, also notifying the account-holder of the assigned account number. Each day, e-gold's due diligence and investigative staff screens all accounts created since their previous screening session to locate accounts with false or inadequate contact information. The screening is assisted by a series of pre-configured database queries that flag suspicious patterns that have been found to be associated with false information. Accounts suspected of false identities are immediately blocked, rendering them incapable of receiving e-gold transfers.

Whenever a transaction occurs or a user update of contact information is committed to the database, the system captures a permanent record of the IP number and timestamp. This vital data is key to investigative techniques that require linking accounts in a constellation quietly controlled by a single entity seeking to mask their identity.

In 2004, e-gold implemented a countermeasure to mitigate phishing exploits (a form of identity theft). The e-gold system keeps track of the IP number and browser agent data from which a user logs into their e-gold account. If a login attempt is made from a different IP number or computer, the system will not allow access and will issue a challenge, e-mailing a one time PIN to the e-mail address registered with the account. This e-mail serves the dual purpose of notifying the rightful user of an unauthorized attempt to access their account and alerting them to the fact that their account information may have been compromised. The system also captures a permanent record of the IP number from which the attempt was made.

e-gold users are encouraged to supply complete and accurate information when they establish their account and to update their information if the contact data does change. If an account holder loses their passphrase, this contact data is required before a new one will be issued.

Of particular importance is e-gold's Right-of-Association in the e-gold User's Agreement. e-gold reserves the right to refuse to do business with individuals and entities at the sole discretion of e-gold. This right enables e-gold, Ltd. to refuse an active account to any entity suspected of engaging in illicit activities. This right is imposed by blocking the suspected account, preventing it from receiving transfers. Blocking an account still allows a user to spend the existing value in their account. A feature implemented in 2005, however, enables account users to refuse to accept Spends from blocked accounts. In the case of suspected child pornography, accounts are frozen outright, pending full investigation, thereby stopping all account activity.

e-gold has initiated a major system improvement to change from an account-based login process to a user-based login. With the implementation of this change e-gold will dramatically streamline the ability to capture only accurate user identity information and further reduce the already poor hospitability of e-gold for illicit activity. This change is significant requiring substantial programming and implementation switchover processes, and is expected to be deployed early in 2007.

#### **e-gold is not a major payment system for Child Pornography**

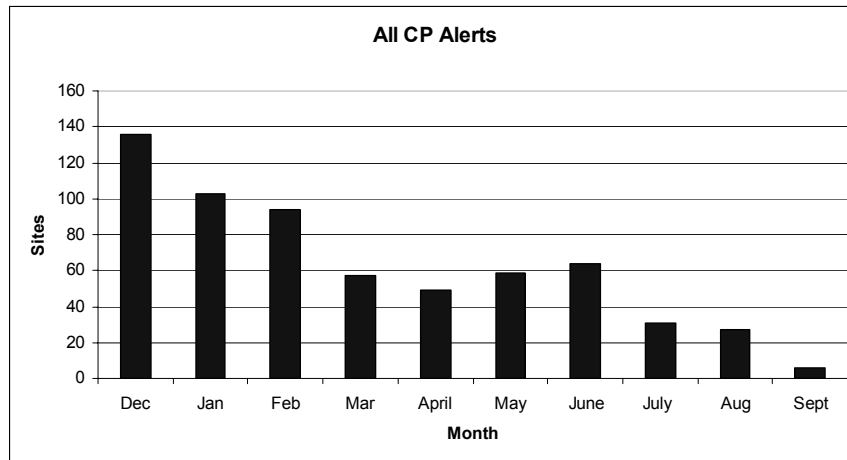
e-gold first experienced the possible use of e-gold for CP payment in early 2003. Those indications proved to be "phishing" sites using the bait of CP to learn account data of e-gold users, suggesting CP availability though apparently not actually selling it. e-gold blocked those accounts from further use of e-gold as well as all associated accounts.

At the beginning of 2004, e-gold investigators received a small number of third-party reports that proved to be real cases of CP sites accepting e-gold. As these sites were identified, they were blocked, along with all associated accounts. Recognizing the problem was real and growing, e-gold began to reach out to third-party watchdog organizations to help in the alert process. This reaching out was frankly very difficult: e-gold was not well known or understood, and often, responses from these third parties were limited. e-gold did increase its in-house investigative activities and continued efforts with law enforcement. In mid 2005, the National Center for Missing and Exploited

Children initiated their work that led to this financial coalition, which has helped significantly. e-gold is very proud to be one of the founding members of this very worthwhile coalition.

During this time period, e-gold received adverse press that came close to implying complicity in this problem, but it was press that was not justified. Based upon the financial size of the CP trade identified by the NCMEC and our review of historical transactions, e-gold has been the payment mechanism abused in less than one hundredth of one percent of the CP payment dollar volume since this problem surfaced. The NCMEC CyberTipLine sends alerts to Financial Coalition members, and alerts are received from other third-party sources as well. Since collaborative efforts started, the activity has decreased dramatically. When an alert is investigated, 95% of the time the account has already been identified and blocked through e-gold's own internal investigative efforts, almost always detected upon the first payment or before a single payment has been received.

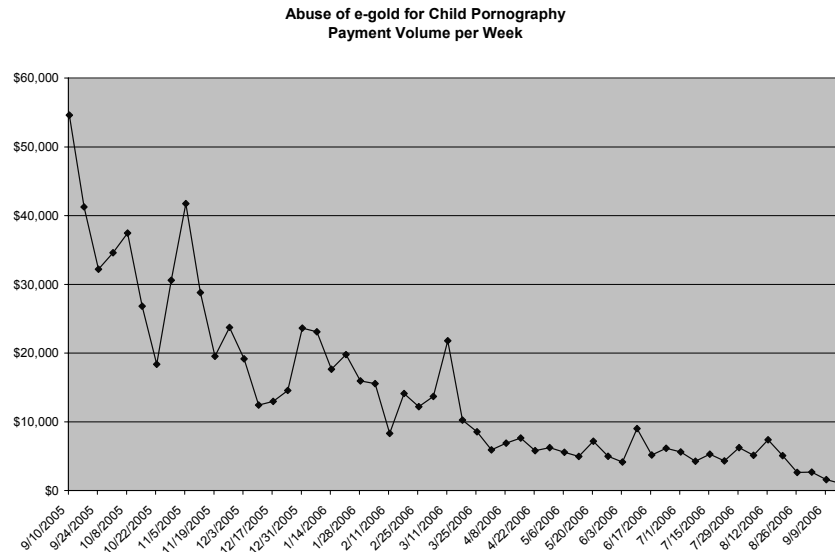
The following chart represents all CP alerts from all sources since December 2005.



e-gold investigators estimate that 90-95% of the alerts received are for CP websites for which e-gold has already blocked the applicable account.

The very favorable trend shown in the chart is not an accident. e-gold continues to refine its protocols to detect and interdict CP payments. Investigative protocols are routinely upgraded as more is learned about the behavior of the perpetrators and enormous personnel resources are applied. e-gold's cost for investigative and preventive actions to stop the use of e-gold for illicit activity, especially CP, is the single largest element of expense in its business. e-gold will continue to apply this attention and resource until the problem no longer exists.

The following graph illustrates the declining dollar volume that, unfortunately, has escaped detection before the accounts were ultimately identified and blocked. It is evident that the visibility we gained from our association with NCMEC in the fall of 2005 was a turning point in our efforts to prevent e-gold being used at all for CP payment. The declining value depicts the evolving capability of our investigative techniques and show we have reduced e-gold abuse to a marginal level.



e-gold is not limiting its efforts to its own data base. Whenever a CP buyer account is identified, e-gold investigators alert the exchange provider from whom the perpetrator purchased their e-gold. The exchange providers are proving very helpful in suppressing CP from the demand side. It has been highly encouraging to see how strongly these organizations are supporting efforts to deter this crime.

As low as the escape payments have become, we will still remain vigilant: we know full well that these criminals will not stop until the risks of their activity outweigh any possible commercial incentive. We will continue to strenuously support the NCMEC and law enforcement until the problem is gone.

#### **Justice Department Investigation**

In a spirit of full cooperation and disclosure, it is fair to inform the Committee that Gold & Silver Reserve is under investigation by the United States Justice Department. G&SR remains confused as to why this investigation was undertaken, why it continues, and why G&SR and its founder, Dr. Douglas Jackson, have been treated in such an abusive manner.

In December of 2005, the Secret Service conducted a “raid” of the Gold & Silver Reserve offices and Dr. Jackson’s home. Bank accounts were frozen, and company funds were seized. In an emergency hearing in U.S. District Court on January 13, 2006, the freeze order on Gold & Silver Reserve’s bank accounts was lifted. Though numerous criminal claims had been made in obtaining the search and seizure warrants, the government made no attempt to sustain such allegations. The only claim at that time and continuing now is a contention that G&SR is operating as a currency exchange without the proper license. G&SR had previously proposed to the Government that e-gold be classified for regulatory purposes as a currency, enabling G&SR to register as a currency exchange. In a Treasury report released January 11, 2006, however, the Department of Treasury reaffirmed their interpretation of the USC and CFR definitions of currency as excluding e-gold.

As early as 2001, Gold & Silver Reserve attempted to make contact with the United States Secret Service to explain how the e-gold system works and to illustrate the advanced protocols for interdiction and investigation of potential criminal use. Dr.

Jackson, e-gold and Gold & Silver Reserve's founder and CEO, scheduled meetings to meet with the Secret Service in Washington—meetings which were postponed and subsequently canceled by the USSS. These rebuffs by the Secret Service continued during the time period when an investigation of the Shadow Crew, a carder ring, was made public approximately a month before the raid. At no time did the Secret Service engage with e-gold investigators, even though the company volunteered to assist the Secret Service by obtaining information to assist in their investigations under proper subpoena. Throughout this period, Gold & Silver Reserve cooperated with numerous other U.S. and international law enforcement agencies and expeditiously answered subpoenas.

G&SR, for nearly a year, had been engaged with an agency of Treasury in a BSA (Bank Secrecy Act) compliance examination it had voluntarily initiated for the purpose of determining how Gold & Silver Reserve, Inc. should be regulated.

In order to obtain the subpoena allowing the search and seizure in December, it would also have been necessary to show the court that there existed a high probability of flight or destruction of records. Dr. Jackson, his wife, and their two children have lived in Melbourne, Florida for the past 14 years. Gold & Silver Reserve has regularly cooperated with all law enforcement in the United States as well as with non-U.S. governments, regularly providing information to law enforcement under due process. As noted earlier, Gold & Silver Reserve had contacted the Secret Service repeatedly to explain the system, the data it held, and how Gold & Silver Reserve and law enforcement could cooperate.

Online payment systems, credit cards, money transfer systems, and banks are all subject to attempts by criminal elements to use them for moving illegally obtained funds. No one is exempt from the threat. Extensive public scrutiny has recently been provided to a U.S. government program to review international Swift transactions of major financial institutions, a program seen as important and necessary, looking for money laundering activity. In the Shadow Crew case itself, public pronouncements identified other systems, including well-known PayPal and Western Union. From Gold & Silver Reserve's own investigation, it is certain many large U.S. banks have had illegal funds processed into and out of their accounts. Gold & Silver Reserve does not know why it has been singled out for investigation when the other larger institutions have not, especially considering Gold & Silver Reserve has possibly the best ability to track payments and identify those making transactions and had made repeated offers to assist if provided with proper legal direction.

In December 2005, the Secret Service confiscated all records and documentation from the e-gold system and Gold & Silver Reserve's offices. It has the entire history of every e-gold transaction ever made. As of December, e-gold had processed over 55 million individual financial transactions—the greatest majority from U. S. citizens. Since the December 2005 government actions, e-gold has cooperated fully with the government. Despite the fact that the U.S. government has all the records, Gold & Silver Reserve has continued to support government investigations and respond to individual subpoenas. This assistance includes supporting an investigation of this same carder ring by other agencies of the U.S. government.

Gold & Silver Reserve regrets being in this conflict situation with a service of the United States government and does not understand why. Seized funds continue to be held, pending what appears to be a never-ending investigation we now believe to be over two years long. These funds were designated for ongoing improvements of the e-gold system, which would have the effect of making the e-gold system even less hospitable for criminal abuse. Employees and contractors of Gold & Silver Reserve have had their lives interrupted, being called from Florida to Washington for testimony, having never been interviewed previously. The ongoing legal issue is depleting resources for Gold & Silver Reserve's defense against apparently uncertain claims since the Government itself has deemed e-gold not a currency, thereby rendering the claim of not being licensed as an

exchange service unfounded. e-gold continues to labor under a cloud of unwarranted suspicion, which is clearly impacting business operations and its ability to reach out with marketing initiatives to natural strategic partners, such as the very financial institutions that participate in this coalition.

Gold & Silver Reserve hopes this issue is settled quickly, that seized funds are returned, and that proper attention be given to the investigation, apprehension, and prosecution of the criminals now operating at will. G&SR will continue, as always, to obey the law and support law enforcement through every possible means to stop true criminal activity.

### **e-gold's Future**

e-gold, despite unwarranted adverse press and intense government investigation, is remaining true to its initial vision. With the ever-increasing online commerce and globalization, the need for a cross border, risk free, low-cost payment and remittance system is growing. The ability to provide a service to individuals from all backgrounds and economic conditions will serve to simplify increasing world commerce and allow the migrant worker to perform his business in one country and then buy goods or send money home across a border easily and inexpensively. This ability can only serve to bring all the economic interests and people across the world closer together.

Historically, e-gold has been viewed by some as presenting a potential risk, possibly facilitating improper cross border movement of funds. It has been difficult to fully educate everyone involved in a rapidly changing economic online world. This risk, however, is clearly not the case. It is more important that a proper focus be given to e-gold's ability to better monitor and control those cross-border transactions while providing enhanced service to individuals.

Multiple U. S. government agencies could benefit from using e-gold, including the U.S. Postal Service, the Internal Revenue Service, and the U.S. Mint. Low transaction fees, finality of settlement, and transaction traceability are all positive features supporting agency adoption. For example, the U.S. Postal Service deals in Postal Money Orders and a cross-border remittance program. The inherent risks of money laundering would be significantly reduced by encouraging a combination of the USPS' over-the-counter cash functions with the flexibility of user-directed transfers via e-gold. Rather than outlawing informal value transfer systems or leaving the unbanked no alternative to monopolistic remittance processors, this flexible combination with permanent records on a single database would capture significant market share while eliminating a potential channel for terrorist funding or money laundering.

### **Summation**

e-gold is a business, but within its mission is also a fervent desire to bring a benefit to the world. It is not now nor ever has been a suitable vehicle for persons engaged in illicit activity. With the full cooperation of law enforcement, e-gold is, in fact, one of the least hospitable systems a criminal could use. The NCMEC's Financial Coalition is demonstrating how a strong level of cooperation can lead to the reduction and, hopefully, elimination of crime on the Internet.

It is certainly e-gold's objective, working with the NCMEC and our coalition partners, to completely eradicate child pornography on the Internet.

Again, thank you for the opportunity to participate in your Committee's hearings. We remain willing to help in any manner possible.

MR. WHITFIELD. Thank you very much for all of your testimony. Dr. Jackson, I will start with you because to be truthful, I have not really been aware of digital currency for a very long period of time, but when I

do hear about digital currency I do hear those words, anonymous and untraceable. But you are refuting that, and it is your position that that is not the case. Is that my understanding?

MR. JACKSON. That is correct. Like in this particular area there is concern with the buyers, and there is concern with the sellers of these materials. Now there is a disparity between them. The sellers, the ones that survive and remain online, they are very good. They are world class experts in concealing their identity. We know a great deal about them, and have interfaced with law enforcement. We know what country they operate out of, and it is quite possible that they will soon be apprehended. The buyers, however, are total amateurs when it comes to trying to conceal their identity. If you want 3,000 conformed identities of United States citizens that have made these sort of purchases find the appropriate way to service with the request for information and it is yours. If you want additional information on another 2,000 individuals in Australia, the UK, German, Japan, we have that information as well.

MR. WHITFIELD. What due diligence do you undertake before you open an account?

MR. JACKSON. Here is where it gets confusing. We are different than the card processors. Our investigative tools are database. We have a permanent record of every transfer that has been made back to, well, since 1996, including let us call it forensic information that is made a permanent record by the direct interaction of the user with the database.

MR. WHITFIELD. And where is that permanent record located?

MR. JACKSON. It is on our database servers in the United States. Let me try to clarify that part because this may be technically difficult. As an illustration we had an inquiry this week from SEOP, the agency in the UK. Their question was, well, you have identified Mr. So and So as a purchaser of hard core pornography. How do you know that he has done this? And when I reviewed our answer, it required five dense paragraphs of technical jargon and it could be baffling to people to understand how we can know so much about people from a consolidated database.

MR. WHITFIELD. Well, what about due diligence on the merchant side?

MR. JACKSON. We make no distinction between a merchant and a consumer where a merchant is somebody that can receive payment, and a consumer is somebody that makes payments. That doesn't exist within our system. Every account has the capability to make and receive payments to have the efficiencies of automation interfaces and so forth. I believe what you are asking is the sort of information that we gather on account creation. There we require the individual to give us a contact name and address, telephone number, and an e-mail address. At the

present time, we don't verify any of that data except for the e-mail address.

However, it is very much in the interest of the user to supply correct information. Where the rubber tends to meet the road is in the event that somebody has bobbled their password or in some way needs to reacquire access to their account they contact customer service, and it is that contact information that enables them to re-establish contact with the account. In the majority of cases though people simply provide correct information. In the instance of an investigation, however, it doesn't matter if somebody has provided false information because of the fact that unlike every other payment system in the world, the end user directly logs in and is interacting in the database in a fashion that leaves behind what are called forensic scruff. That is the sort of clues at the low tech end, items such as their ID number, but other identifying factors that enable us to link up a constellation of accounts that may belong to the same entity and ultimately connect them up with a true identity.

MR. WHITFIELD. Now how do you know that most people provide correct information?

MR. JACKSON. Well, focusing particularly in this category of crime not uncommonly we called them up and told them that they must not do this anymore, that we know what they are up to.

MR. WHITFIELD. Well, I have some other questions for you but I need to move on. Mr. McCarthy, I have here an e-mail between you and Kelli Andrews on our staff, and it talks about the number of new child pornography sites being identified that say they accept Visa, actual or just displaying your mark, and it says that they are decreasing. In 2005, for example, there were 132 sites. And then you had mentioned in this e-mail that you retest the sites that you have identified as child pornography and those that say they are accepting Visa, and 91 percent of those that you retested are now not using Visa, but what about these other 9 percent that say they are still using Visa? I think you have had an opportunity maybe to look into this. Could you elaborate on that for us?

MR. MCCARTHY. Thank you, Mr. Chairman. We have an internal program that is designed to measure the effectiveness of our steps to remove the Visa brand from the websites that are engaged in child pornography. And the numbers, they show a decline over time in the numbers that continue to maintain the Visa logo on the website, so the most recent numbers from 2006 show that if you look at the websites that we have originally identified as purporting to accept Visa and then retest those sites, 5 percent of them still have the Visa logo appearing on it.

We have done additional research into that area to look at that and our search firm completed a sweep in the last week to look at the number of sites that are actually present in the Visa system during the retest



,because what these numbers indicate are not the ones that are actually in the system, it is the ones that are purportedly in the system. Just last week the search firm looked at 3,700 sites that had been in their data bases that at some time or other had accepted payment cards for child pornography purposes. That includes Visa, MasterCard, PayPal, and a number of other operations as well. They found of the ones that had originally been identified 25 sites that were originally identified as involved in child pornography still maintained a Visa logo on the website.

They were able to do a transaction involving a Visa card with only 10 of those sites. The other sites, even though they purported to be accepting Visa cards you could not even do a test transaction on the website.

MR. WHITFIELD. So we are talking about maybe around 12 sites in 2005?

MR. MCCARTHY. Let me just finish the data dump because this is the number I want you to focus on.

MR. WHITFIELD. Okay.

MR. MCCARTHY. After they did the test transactions on those 10 sites they found 25 that had been able to be identified as perhaps using Visa cards. Ten they did the test transactions on. They found one site that was actually accepting Visa cards.

MR. WHITFIELD. Okay. So you are saying in 2005 of the 12 sites that were still in operation after detected that it was a child pornography site using Visa that after you did the re-test, only 12 sites were still accepting Visa, and is that what the situation is?

MR. MCCARTHY. There is a series of confusing measurement concepts here. The important measurement concept that those numbers that you have relayed to is not sites actually accepting Visa cards. Those are sites that appear to be accepting Visa cards. The logo is on the site.

MR. WHITFIELD. Okay. So what you are saying, these sites appear to be accepting Visa?

MR. MCCARTHY. The logo is on the site or they say please enter your Visa card number to make a purchase.

MR. WHITFIELD. Okay.

MR. MCCARTHY. When you look at those sites upon retest you find that 5 percent of the original sites still claim to be accepting Visa cards. When we did our real test last week with our search engine you went from 25 sites that said they would accept Visa cards to 10 tests that we were able to perform. We couldn't even perform the tests on the other 15. And only one of the sites was actually accepting Visa cards at that point.

MR. WHITFIELD. So you are saying that of these 12 sites or so only one are still accepting Visa so why would you--

MR. MCCARTHY. It is even worse than that. Of all the sites that have ever been investigated by our search firm, 3,700, they have looked at those sites over the last several years. They have found only one site that has been still in the system after all these years.

MR. WHITFIELD. And what site is that?

MR. MCCARTHY. The name is irrelevant. We immediately notified the acquiring bank about the problem. It was not an acquiring bank in the United States. It was outside of the United States and it will be shut down.

MR. WHITFIELD. It will be shut down.

MR. MCCARTHY. Yes.

MR. WHITFIELD. All right. Mr. Sullivan, since a PayPal account must be backed by financial instrument, usually a credit card or bank account, explain the benefits of opening a PayPal account rather than using a credit card.

MR. SULLIVAN. Certainly. And every account would need to be backed by a credit card or a bank account. PayPal emerged in the late '90s as a means for small businesses and individuals to make payments on the Internet. In particular, it grew out of the eBay environment, and if you think of an eBay transaction, I personally list items for sale on eBay, and when I list an item on eBay it is available to the world to purchase. I want to be able to accept payments from anyone on the Internet. Before PayPal came along if you were the purchaser of my item you would have had to write a check, take it to the bank account to take it to the post office and mail it to me. I would have to receive it, deposit it, wait till it cleared.

With PayPal you could then take the money from your bank account using PayPal, have PayPal transfer it to my PayPal account and then I could move it into my bank account. And so it brought efficiency to a very inefficient process.

MR. WHITFIELD. My time has expired. Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman. In listening to the testimony here this afternoon, I would believe we would have no trouble with child pornography because you all are doing such a wonderful job, but the facts belie the fact of the testimony. You say look for child pornography, if you use those words on the Internet you aren't going to find any because no one uses those words. And if you terminate all transactions that could be child pornography, how do we get to the point then where we are at \$21 billion a year, three times greater than downloading music. Music is a legitimate business on the Internet and that is \$7 billion. Child pornography is estimated to be \$21 billion. If

we are all policing the Internet so wonderful, how does it happen then? How do we get \$21 billion? Anyone want to take a stab at that?

MR. JACKSON. Does it occur to you to question that number?

MR. STUPAK. Pardon?

MR. JACKSON. Does it occur to you to question that number?

MR. STUPAK. Yes, we have, a number of times. This is our sixth hearing, and we have gone over those numbers quite closely.

MR. JACKSON. We can account since the dawn of time for about \$3 million.

MR. STUPAK. That is just you.

MR. JACKSON. Yeah.

MR. STUPAK. All right. Did you shut down Child Dreams--Children Dreams, I mean, that has your gold--

MR. JACKSON. We shut them down about twice a day.

MR. STUPAK. Your e-gold on there.

MR. JACKSON. We find them about twice a day and shut them down either before they receive a payment or upon their first payment.

MR. STUPAK. As testimony was even earlier today too, you said you find two a day. No sooner do you shut one down and another one pops up just under a different name. So I guess my question would be you have these Web crawlers. How often do you require your Web crawlers to update the terminology and the characteristics they are using to identify pornography sites, once a year, once a week? Anyone want to answer that?

MR. JACKSON. Is the question directed to--

MR. STUPAK. Any one of you.

MR. JACKSON. Okay.

MR. STUPAK. Do you use Web crawlers?

MR. JACKSON. At this point things are suppressed down so low each individual case that escapes, each individual payment, enables us to review it against our protocols and see if a change of protocol is needed. A year ago--

MR. STUPAK. I am talking about Web crawlers that look for pornography sellers.

MR. JACKSON. We don't use Web crawlers. We don't need Web crawlers. We have no idea--

MR. STUPAK. Then don't answer my question. Let me ask someone who uses a Web crawler then.

MS. GOLINSKY. I can answer the question. For MasterCard we are changing the lexicon to terminology constantly. We are looking at the Web 24 hours a day.

MR. STUPAK. How often do you change it then?

MS. GOLINSKY. How often are we changing the words that we are using?

MR. STUPAK. Yes.

MS. GOLINSKY. It is an iteration process so the company that we use that does this for us. They are constantly learning and trying to keep ahead of what the terminology is and changing it as they know that it is changing.

MR. CHRISTENSON. And, Congressman, the same is true of American Express.

MR. STUPAK. They tell us that on websites now if they don't use any terms but a picture there is no way to determine that, right? You can't determine that as a pornographic site or a possible pornographic site. Anyone want to answer that? The Web crawlers somehow can't detect that.

MR. CHRISTENSON. The Web crawlers normally key off of key words.

MR. STUPAK. Right, not off of a pictureb so if I just have a picture up there.

MR. CHRISTENSON. I am not a technologist. My understanding is that you would have to actually download the picture so that you could search the Web looking for a match of that picture. Otherwise, they would have to be looking for words.

MR. STUPAK. Correct.

MS. GOLINSKY. But the Web crawlers are not only doing word searches but also looking at a million pages a day so they are doing both.

MR. STUPAK. Sure. As long as it is like Joel and then there is a picture, we are not picking that up is what they are telling us because the Web crawlers can't pick up the borders of the photographs.

MR. CHRISTENSON. One of the advantages, I think, of the Financial Coalition is that you have two different things going on. A lot of the companies will use these automated searches of the Web that can cover millions of pages a day. The Cyber TipLine is based on people who call in or e-mail in information that they come across through the human search of the Web so we are having now the National Center reporting to all of us information they come across which could just include a picture in addition to the Web crawlers that we are using.

MR. STUPAK. Well, the National Center, did they not, Mr. Christenson, give you 24 referrals this summer to investigate?

MR. CHRISTENSON. That is right, and as part of the test period they passed on 24 websites.

MR. STUPAK. What would happen on those referrals? How many child pornography sites have you found?

MR. CHRISTENSON. Well, as I detail in my written testimony by the time we got down to actually finding a site that accepted American Express card, we were down to one site which we immediately terminated and reported back to the National Center and to law enforcement on that.

MR. STUPAK. What happened on the Landslide case then? I guess that involved American Express cards without any independent due diligence. Apparently the owner of the Landslide was merely asked whether or not they wanted to add the American Express card by his bank and so how does your system prevent that from happening? If I am a customer and my bank says, here, do you want to use American Express, how would you make sure I am using it then for proper purposes and not improper purposes?

MR. CHRISTENSON. As I detail in my testimony, when someone sends in an application we have a whole due diligence at the beginning to look at a number of things. And then we also have an ongoing search of the Web so that we can find out if they are violating our contract in what they are putting up on the Web and trying to sell. The Landslide case goes back a number of years. We terminated that merchant in February of 2000. And so some of the iterations we made and the improvements in our processes have taken place since then.

MR. STUPAK. American Express, Visa, or MasterCard, if my bank where I am doing my banking gives me the credit card you still have responsibility then to review how that card is being used and make sure it is being used properly?

MR. CHRISTENSON. Absolutely. In the American Express model, we may have some people who will refer us applications, but it is our responsibility to review the application and to decide whether to sign a merchant up or not.

MR. STUPAK. And I take it that wasn't done in the Landslide case then?

MR. CHRISTENSON. I don't know any particulars on that.

MR. STUPAK. Is there--let me ask you this, anyone of you, if you would like. Is there any way to even know whether MasterCard or Visa or American Express could be given as a gift card, how would you handle that? You know, gift cards seem to be the new rage. How would you handle that? I could use it then--they are already issued, right, and it is like prepaid so you can't really monitor that, can you?

MR. MCCARTHY. Mr. Stupak, can I answer that?

MR. STUPAK. Sure.

MR. MCCARTHY. The gift card that Visa has--gift cards I think all of the other payment mechanisms here have gift cards, they turn out to be part of the solution in this area. We have provided to the law

enforcement officials at ICE 100 of these prepaid cards for their use in tracking down the child pornography merchants on the Internet. When they are trying to find out the name of the merchant, they do a test transaction. The test transaction can then be tracked in any one of our payment systems. We can go back through our records and find the bank that is associated with the transaction.

MR. STUPAK. But those are the cards given to law enforcement.

MR. MCCARTHY. These are regular, ordinary gift cards that are provided--

MR. STUPAK. But you would have all those numbers beforehand. How would you stop me from using one of these cards? How would you--

MR. MCCARTHY. In the context in which we are working with law enforcement right now the major effort is to identify the Web merchant and those prepaid cards are useful in identifying the Web merchant. For technical reasons it turns out to be slightly better to use a gift card than it is to use a debit card or a credit card to identify the merchant in the system. And so that is the function that those cards are being used for right now by ICE under the law enforcement agencies. We delivered 100 of them 2 weeks ago to the ICE personnel for their use in this area.

MR. STUPAK. So this is just an experiment you are starting then? You started it a week ago, right?

MR. MCCARTHY. Those are the cards that we use in our own test transactions. We are sharing them now with law enforcement for them to use in their transactions as well.

MR. STUPAK. What I still don't understand, and maybe I am missing it, if I get a gift card, Visa gift card, and I use it, how is that going to-- how are you going to discover that?

MR. MCCARTHY. In many cases gift cards are traceable. They are reloadable cards.

MR. STUPAK. Traceable to who? How would you know? Wouldn't the purchaser be anonymous?

MR. MCCARTHY. I got one that I give to my kid and it is a Bucks card. He has to fill out an application. I have to sign for it. They know who has got that card. If the card is not reloadable, it is an anonymous card, then that kind of information isn't available. But the point is that on the merchant side it is those cards that are the most useful to find the merchant. And when law enforcement comes to us what they are asking us almost all the time is to help them locate the merchant.

MR. STUPAK. I agree giving a hundred to law enforcement because you have the numbers there and you can track it, but if I get a gift card how would you ever know who owned it to begin with? You wouldn't, right?

MR. MCCARTHY. Some gift cards are anonymous. Some of our programs have anonymous gift cards. Many other programs use anonymous gift cards.

MS. GOLINSKY. Congressman, if I may from a MasterCard perspective.

MR. STUPAK. Sure.

MS. GOLINSKY. For our gift cards, stored value cards, we generally require the issuers who issue those cards to conduct the same sort of due diligence and know the requirements they would for any other program. With respect to--

MR. STUPAK. Yeah, but require due diligence if I fill out one of these gift cards and I give it to a friend and he uses it wrongly, how do I have responsibility for I gave it to that friend?

MS. GOLINSKY. I hear what you are saying, but what we do is we make sure that we track any sort of program that we have in our system. Our rules apply to all of our cards whether they are stored value cards or credit cards or debit cards except in limited instances where we are talking about low value dollar cards that cannot reloadable we require customer identification. That is, you can trace it to someone. It might not be the person who you gave that card to cannot be traced in the system. Our efforts right now are focused on taking away the ability to use our cards period, regardless of the type of card to be used.

MR. STUPAK. One more, if I may, Mr. Chairman. How long do you retain your records, your financial transactions?

MR. CHRISTENSON. We retain records 7 years.

MR. STUPAK. Seven years. Is that IRS requirement or so?

MR. CHRISTENSON. Pardon me?

MR. STUPAK. Is that an IRS requirement?

MR. CHRISTENSON. It is a little bit beyond what the legal requirement is.

MR. STUPAK. Okay. Because it is a big issue up here how long ISPs and do we apply that same standard to financial institutions. Seven years is about right too for MasterCard?

MS. GOLINSKY. Congressman, I would have to get back to you but it is several years.

MR. STUPAK. How about you, Mr. Sullivan, on PayPal?

MR. SULLIVAN. Minimum of 2 years.

MR. STUPAK. Minimum of 2 years. Okay. And, Mr. McCarthy.

MR. MCCARTHY. We retain their records for years, but the real point is that we turn over information instantaneously to law enforcement. It is not as though they are coming after us for a transaction that is a year or two old. We get it to them right away when we see the problem.

MR. STUPAK. Mr. Jackson, Dr. Jackson, how long do you keep your records?

MR. JACKSON. Forever.

MR. STUPAK. You said since 1996 or something I think you said in your--

MR. JACKSON. Well, that is our forever.

MR. STUPAK. Thank you.

MR. WHITFIELD. I think all of us are quite aware of the difficulty in dealing with this issue, and there are so many different aspects of it, but as you listen to American Express and MasterCard and PayPal and whatever, we know that there is a lot of due diligence that is conducted before you sign up a merchant or your acquiring banks sign up merchants. In the case of American Express you do it yourself when you look at credit histories and you get a lot of information and so forth and so forth. And then all of you seem to be going back and you monitor websites periodically, merchants that you are dealing with. Is that accurate? That is sort of a layman's statement. Overall that is pretty accurate, isn't it?

But in your case, Dr. Jackson, the clear sense here is that you don't really distinguish between a merchant and a buyer. You just have an account and you can deal with it any way you want to. I get the impression that there is not a lot of due diligence in the sense of looking at credit histories and ongoing monitoring of websites of people that have accounts with you. Would that be accurate or am I inaccurate in that?

MR. JACKSON. It is difficult to compare e-gold with Legacy Payment Systems. The nature of the transaction, it will confuse people. Let us say, for instance, that you create an account and you are trying to demonstrate some thesis like, oh, look, this is anonymous. And so you create an account with nonsense information. What you have is an empty account that is going to remain empty with no value forever. Now the logic that makes e-gold extremely traceable is twofold. One, it is a closed system unlike every other payment system in the world which is an extension of existing banking mechanisms. E-gold is completely independent. It is a closed universe, a closed universe of value backed by gold.

To send value into the system is impossible for the user. Now combined with that inability to add value to the e-gold universe is the fact that every transfer value within the universe has a permanent record, and so it is like touching a spider web. If you have that empty account that is going to remain empty forever, the only way we will ever have any e-gold is to receive a payment from somebody that has already got some, thereby creating a permanent discoverable linkage to that person



so you can trace the lineage of every particle of value back to Adam and Eve or more relevantly back to perhaps an exchange entity who may have bought or sold e-gold.

That person will have very good reason to keep track of the identity of their customer because they may accept payment through one of the other payment systems represented here which are highly reversible and therefore they have an extreme need to know who they are dealing with in case a person tries to stiff them or reverse the payment. And so we work in complement with the exchange services sometimes for flushing out the identity. Even though these exchange services are independent of e-gold and competitive with one another it is the virtual equivalent to a worldwide network of agents that have supplemental information regarding the identity of these users.

MR. WHITFIELD. The bottom line is it appears to me that if I am a person dealing in child pornography or using a site and have subscribers that are paying for viewing child predator type scenes it would be much easier to use your system, much less traceable to use your system than any of these other systems. But I would ask you, Mr. Christenson, would you agree with my assessment knowing what you do about digital currency or would you not agree with it?

MR. CHRISTENSON. Well, I am no expert on digital currency, but I would say that we do quite a bit to understand both who the merchant is and who our cardholders are, and so you have to provide a lot of information. You are going to look at your credit records. You are going to have to confirm location and all those kind of things. So we do a lot of due diligence to know our customers, and I think that that has a big impact when you then find somebody who is involved in illegal activity. You can quickly follow up on who those people are.

MR. WHITFIELD. Ms. Golinsky, what would you say of the statement I just made, is that a fair statement or is that not a fair statement?

MS. GOLINSKY. Mr. Chairman, like Mr. Christenson I don't know enough about digital currency. I will tell you that it is something in terms of the sales on the Internet it is something that MasterCard is looking at, but I couldn't say more about it because I don't understand how--

MR. WHITFIELD. What about you, Mr. Sullivan, do you have any comment?

MR. SULLIVAN. I am afraid I too am not an expert on e-currencies.

MR. WHITFIELD. And, Mr. McCarthy, what about you?

MR. MCCARTHY. I am going to take a pass as well, Mr. Chairman.

MR. WHITFIELD. Okay. Well, Dr. Jackson, I have here some featured sites off of your website, off your e-gold directory. And it has,

for example, getafreelancer.com, hushmail.com, mozilla.org, agentgold.com. I mean what can you tell us about--I got eight pages of these. Do you have detailed information on all these?

MR. JACKSON. Absolutely. The people that are linked on the website, of course we have certainty of knowledge as to every detail of who the company is and the principals.

MR. WHITFIELD. So you would have information about the principals for every one of these sites?

MR. JACKSON. Certainly.

MR. WHITFIELD. Did you do a credit check on that?

MR. JACKSON. No, because unlike every other payment system here we are absolutely immune to the credit risks of the users, which is an important point to understand. This is part of why we are going to bring benefits to this economy. Every other payment system if a user defaults somebody is going to pay the price. Typically that loss is to be passed through to the end recipient who will have the payment sucked back from them. Since default cannot happen in the e-gold system there is no element of credit. It is on a strict debit basis.

MR. WHITFIELD. How do you know if these businesses are legitimate or not legitimate?

MR. JACKSON. We do not vouch for their so-called legitimacy, but what we do know is who they are. Of course, if we were to hear some sort of a complaint regarding them they are going to be pulled from the website. But in the absence of that complaint we are content to simply know their identity. Now we have of course debated as to whether it is appropriate to continue to even list links to sites since the fed doesn't link sites that accept dollars, and at some point we are going to move away from that model as it becomes more ubiquitous.

MR. WHITFIELD. Now I have been told that the exchanger for e-gold is in the U.S., but everything else is outside the U.S. Is that a true statement or not?

MR. JACKSON. The e-gold system, everything about its setup, its governance model, is designed to serve the dual imperatives of freedom from default risk and finality of settlement. Before e-gold the only institutions in the world that could claim to attain those attributes were government central banks. In many regards we are modeled after the Federal Reserve with its fed wire settlement platform, which is a real time gross settlement platform. Now to try to achieve freedom from default risk, we have to look at every category of threat that could intervene that could cause e-gold to fail in its contractual obligation to have gram for gram 100 percent backing of physical gold.

One of those elements is a separation of roles between the exchange function, which does entail business risks, and the core functions of settlement and issuance of these liabilities.

MR. WHITFIELD. But what part of your business is in the U.S. and what part is out of the U.S.?

MR. JACKSON. Okay. The central contractor for the e-gold liability, that is, e-gold's obligations are memorialized in the e-gold account user agreement. That is an agreement between the user and the issuer of e-gold, which is a company called e-gold Limited, which is domiciled in Nevis. However, all operational and fiduciary roles for the operation of the system, and those consist of the operator of the Mint, the escrow agent, and in fact the physical entities that perform the repository function, those are all at the moment United States companies. E-gold is operated out of Melbourne, Florida, quite frankly.

MR. WHITFIELD. So it is operated out of Melbourne and then you have part of it in Nevis, is that correct?

MR. JACKSON. The only part that resides in Nevis is it is where the general contractor is domiciled. The wisdom of that decision I think was very well borne out last December when there was a shoot first, ask questions later intervention by an agency of this government.

MR. WHITFIELD. Shoot first, ask questions later, what are you referring to?

MR. JACKSON. It is detailed in the written testimony, but my company, Gold and Silver Reserve, located in Melbourne, Florida, was host to the Secret Service taking all of our books and records, going into Orlando, an AT&T co-location facility where the e-gold and OmniPay servers are located, taking us off line for 36 hours, taking complete record of all these transactions, including those of American citizens back to 1996, invading my home, taking things like my wife's address book, the children's passports, credit cards I happened to leave on the night stand, all of this, based on some sort of a presumption that we are okay with criminal activity, which is quite the contrary to the case.

All we have ever desired is a constructive relationship with law enforcement. We have the same interest as anybody else in rooting out criminal abuse of our system as would any other company in the financial services area.

MR. WHITFIELD. One other question. Ms. Golinsky, how long has MasterCard participated in the MATCH system, and could you describe what this entails for your merchant banks?

MS. GOLINSKY. Sure. I don't know the exact date for how long you participated in it. We are one of the founding members of it. And the way the system works is it is a joint database of terminated merchants that MasterCard runs with other payment networks. So when we have

terminated a merchant or one of our client banks has terminated a merchant for whatever reason, they have to enter that merchant into MATCH and it is a requirement for our banks when they sign up a new merchant that they check MATCH to make sure that they are not signing up a merchant that has been terminated for some reason including illegal purposes.

MR. WHITFIELD. Mr. Stupak.

MR. MCCARTHY. Mr. Chairman, could I add to that? Visa is not an operating partner with the MATCH system, but we have a similar requirement for our banks. If they are going to sign up a new merchant they have to check that database to make sure that he hasn't been terminated in another fashion.

MR. WHITFIELD. Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman. Mr. Jackson, you stated that e-gold doesn't pose a greater risk for use in other financial methods, but yet you will monitor your users and you claim it is not your responsibility to do so. You say you know their identity, but you don't check to see if they are who they claim they are. So how can you make a statement about knowing the merchants you conduct business with when you do no due diligence or oversight?

MR. JACKSON. We have convened this panel today to discuss child pornography, a case study of how extremely effective our investigative techniques are in finding an identified category of crime. The numbers speak for themselves, do they not?

MR. STUPAK. Wait a minute. You said e-gold posed no greater risk for use than other financial methods, did you not?

MR. JACKSON. When I described the default risk, I am talking about what is the possibility that a gram of e-gold would decline in its exchange value--

MR. STUPAK. No, forget the gold stuff. Just answer the question. You stated that e-gold does not pose a greater risk than other financial methods, yes or no?

MR. JACKSON. I guess I don't understand the question. What I was describing was freedom from default. Are you describing in terms of the risk of criminal abuse?

MR. STUPAK. You said to the Chairman, you said you know the identity of all of your users, right?

MR. JACKSON. No. But I did describe extreme traceability.

MR. STUPAK. Okay. How do you identify the person who buys e-gold? How do you identify him? How do you check to see if they are who they say they are? If I say I am Ed Whitfield, how do you check to make sure I am Ed Whitfield?

MR. JACKSON. A person who is selling e-gold--

MR. STUPAK. No, no. I want to sign up for e-gold. All I have to do is go on the Internet, right, do a few clicks and I can register and I can buy e-gold, right? Can I have an account with you?

MR. JACKSON. I am trying to answer your question.

MR. STUPAK. Right.

MR. JACKSON. You can't possibly obtain e-gold from the e-gold company. There is no mechanism for doing that.

MR. STUPAK. I can set up with the company, right?

MR. JACKSON. You need to receive in payment--

MR. STUPAK. And I am backed up by your gold?

MR. JACKSON. --from somebody who already has some.

MR. STUPAK. I can go on there and I can apply to be part of e-gold, right?

MR. JACKSON. Yes, you can create an account online.

MR. STUPAK. I can use your e-mittal pay order, right?

MR. JACKSON. Not unless you have e-gold.

MR. STUPAK. Right. But I can go and sign up for e-gold, can I not?

MR. JACKSON. You can create an account which makes you capable of receiving an e-gold payment.

MR. STUPAK. Okay. My question is how do you know who I am when I sign up on e-gold?

MR. JACKSON. At that point we don't have certainty of knowledge. Now of course--

MR. STUPAK. You have no knowledge of who I am, correct?

MR. JACKSON. --it is a system that is evolving.

MR. STUPAK. Answer the question. You have no knowledge who I am even though I may have the right--

MR. JACKSON. No, the person that has that empty account we don't know much about.

MR. STUPAK. You don't know anything about them. That is--

MR. JACKSON. Well, actually we do know quite a bit. We know the IP number that they created it from.

MR. STUPAK. Sure. You know the IP number but you don't know who that person is.

MR. JACKSON. We have their e-mail address.

MR. STUPAK. I could be a pedophile for all you know or I could not be.

MR. JACKSON. If it is a pedophile and if you are interested in them we can give you thousands of them.

MR. STUPAK. How many--if you can give me thousands of pedophiles, how many of those names have you turned over to law enforcement?

MR. JACKSON. I don't know an exact number. I saw one of them in the newspaper last week.

MR. STUPAK. That your company turned over to law enforcement?

MR. JACKSON. Yeah, it was our bust, but it made it look like e-gold was somehow--it was the typical kind of press treatment where e-gold is mentioned--

MR. STUPAK. I don't care about the press. I just want to know how many have you turned over to law enforcement if you know thousands of pedophiles.

MR. JACKSON. I would need to look that up. The difficulty has been one of jurisdiction, and this has been an area of discussion with the Cyber TipLine when we give a tip about users--

MR. STUPAK. No, no. I am just trying to get these numbers. More than one, more than ten?

MR. JACKSON. I can check.

MR. STUPAK. More than a hundred? Okay.

MR. JACKSON. Probably in the range of hundreds but I could certainly give you an exact number if you would like. The point is we do more to reach out to the buyer than any other system that I know of. The buyer feels the hand of God come down on him right away within minutes after he has done this purchase.

MR. STUPAK. Well, law enforcement, as Mr. Plitt and others have testified, e-gold is one of those that is commonly used by child predators. What active steps have you taken to keep predators from using your technology?

MR. JACKSON. If you are describing the predators as being the purchasers of child pornography--

MR. STUPAK. Yes, or sellers. How about sellers?

MR. JACKSON. The sellers are difficult. There is a handful of sellers, and these people are very capable--

MR. STUPAK. So what do you do to crack down on the sellers of child pornography?

MR. JACKSON. What we do to crack down on the sellers is we find a new account that they create either before it has received its first payment or we detect it upon its first payment. We block it from receiving further payments and we freeze it. If they have managed to exchange value that they received for some other form of payment such as Web Money, we notify Web Money and continue in hot pursuit so they notify law enforcement.

MR. STUPAK. How about Invisible Net where invisibility is the best, how would you stop them from selling child pornography?

MR. JACKSON. I am sorry. Who are we talking about?

MR. STUPAK. One of your customers, Invisible Net. Invisibility is the best defense, it says. So how would you stop them if they were selling child pornography?

MR. JACKSON. If we knew the identity of a seller because we are all looking at the same sellers. There is a handful--

MR. STUPAK. What do you do to verify that Invisible Net is conducting a legitimate business?

MR. JACKSON. We are talking about pornography and what I can do to find--

MR. STUPAK. My question was any legitimate business. Maybe they are selling us--

MR. JACKSON. If there is a staffer that can work with us for some period of time and then he can come back at his leisure and explain it how we find--

MR. STUPAK. Well, you are here today so I am asking you the question. How do you verify Invisible Net is a legitimate company, selling legitimate products, how do you do that? How does e-gold--

MR. JACKSON. All I know about that company is who they are and we have not received complaints about them.

MR. STUPAK. So that is all you know?

MR. JACKSON. If you would like, we can stop linking to any companies on the website. We are not certain that it is of any value, but the point is they are utterly irrelevant to the child pornography discussion. If you want to find child pornography, come to us. We are the world's experts at finding it in our database and we have suppressed it down to the point where it is virtually negligible.

MR. STUPAK. Then you are the world expert, then how many of these illegal sites have been turned over to law enforcement or the National Center for Missing and Exploited Children?

MR. JACKSON. We report to the Cyber TipLine just as everybody else does. However--

MR. STUPAK. How many have you in the last week?

MR. JACKSON. We can find them without ever seeing a site.

MR. STUPAK. Mr. Jackson, how many have you turned in in the last week?

MR. JACKSON. I would have to check.

MR. STUPAK. You don't know?

MR. JACKSON. There are three or four payments that slipped through in the past week. I am not sure that we even know of the site.

MR. STUPAK. Well, you are the first world expert who doesn't seem to know any answers to any of the questions I ask.

MR. JACKSON. Well, I don't think you are understanding me, sir. We don't need to know about the site to find the child pornography. We

can find it in our database because we have such a sophisticated profiling--

MR. STUPAK. Have you done that?

MR. JACKSON. --of the buyers and the sellers.

MR. STUPAK. Have you done that? You said you can go through your database and find those who are selling or buying on your system. Have you done that?

MR. JACKSON. Absolutely. That is what is responsible for this radical drastic decline in successful attempts to buy child pornography.

MR. STUPAK. I will look forward to your answers to the committee on how many you have turned in to law enforcement. You will provide that to us?

MR. JACKSON. Sure. That is fine.

MR. STUPAK. Thank you.

MR. WHITFIELD. I would like to ask the entire panel have you noticed any change in the number of reports that you are sending in to NCMEC, are you finding more, less or about average amounts of reports to the Cyber TipLine.

MR. CHRISTENSON. I would say it is about the same over the past year.

MS. GOLINSKY. Mr. Chairman, I think that we are seeing some reports go down. We have reported approximately 86 sites to NCMEC in the last several months, but I think that as I mentioned in my testimony we are seeing some of our efforts are successful, that we are seeing a lot less direct acceptance of our cards on these sites but we are still making the same number of referrals nevertheless.

MR. SULLIVAN. On behalf of PayPal, I would say that we are seeing a slight decline.

MR. MCCARTHY. It is approximately the same over the last year.

MR. JACKSON. I haven't kept track of information we upload. In terms of alerts that were received from all sources they are plummeting.

MR. WHITFIELD. Dr. Jackson, I would ask you one, do you have a money transmitting license or is that something that you do not feel you are required to have?

MR. JACKSON. There is litigation that is being pursued on this. It is a legal question, and I guess I am hesitant to try to express a legal opinion.

MR. WHITFIELD. But at this time you do not have a money transmitting license?

MR. JACKSON. We have looked at this carefully. We engaged with the BSA group from Treasury approximately a year ago trying to find an appropriate regulatory rubric or an exchange provider such as Gold and Silver Reserve. This group was established to have the competence and



the authority to aid in innovative type of situations where somebody simply doesn't fit into one of the existing frameworks. The difficulty with Gold and Silver Reserve whose activity very much resembles currency exchange is the fact that heretofore the United States Treasury has deemed that e-gold can't really be classified as a currency.

MR. WHITFIELD. Okay. Well, I don't want to get into all of the legal discussions about it. I am just asking a question, do you have a money transmitting license or do you not?

MR. JACKSON. No, because neither e-gold nor Gold and Silver Reserve are money transmitting businesses.

MR. WHITFIELD. Okay. Okay. I want to thank this panel very much for your testimony. We appreciate the work that you are doing, the improvements that are being made, and hope that you will continue to be aggressive in your efforts to curtail this, and with that this panel is dismissed. Thank you. At this time, I would like to call up the fourth and last panel. And on this panel we have Mr. David Strider, who is Executive Vice President, North American Operations for NOVA Information Systems with U.S. Bancorp, and Mr. Ralph Shalom, Associate General Counsel for Litigation, First Data Corporation, Mr. William Matos, Senior Director of Credit Risk, Chase Paymentech Solutions, and Ms. Kim Mowder, Senior Vice President, Bank of America.

Thank all of you for joining us today, and we certainly thank you for your patience. I am sure you have heard more about digital currency than you ever cared about hearing about but as you know this is an oversight investigation. We do take testimony under oath. Do any of you have any objection to testifying under oath? If not, if you would please stand.

[Witnesses sworn]

MR. WHITFIELD. Okay. All of you are under oath now, and we will begin, I will recognize Mr. William Matos for Chase Paymentech for your 5-minute opening statement.

**TESTIMONY OF WILLIAM MATOS, SENIOR DIRECTOR, CREDIT/RISK, CHASE PAYMENTECH SOLUTIONS, L.L.C.; KIM MOWDER, SENIOR VICE PRESIDENT, BANK OF AMERICA; RALPH SHALOM, ESQ., ASSOCIATE GENERAL COUNSEL FOR LITIGATION, FIRST DATA CORPORATION; AND DAVID STRIDER, EXECUTIVE VICE-PRESIDENT, NORTH AMERICAN OPERATIONS, NOVA INFORMATION SYSTEMS**

MR. MATOS. Thank you. Good morning, Chairman Whitfield, Ranking Member Stupak, and members of the subcommittee. My name is Bill Matos, and I am the Group Manager and Senior Director of Credit and Risk Management at Chase Paymentech Solutions. Chase Paymentech is strongly committed to combating child pornography, and it is my pleasure to appear before you today to discuss this important issue. Chase Paymentech is headquartered in Dallas, Texas, and is one of the Nation's largest processors of bankcard payment transactions for merchants.

One of our primary roles is to contract with, and provide services to, merchants to enable them to accept credit cards and other payment methods. Chase Paymentech has a strict prohibition against our services being used in connection with child pornography or any other illegal activity. We have strict standards that must be met before we approve a merchant's application for our services. For example, we collect detailed information about each merchant applicant and thoroughly review the applicant of each potential merchant to insure the merchant meets our credit and risk management requirements.

Not only must we collect information to assess an applicant's credit risk, but we also engage in a thorough review of the compliance risks the merchant may present. Before we approve any applicant as one of our merchants, we must understand the applicant's business model and product line thoroughly. For online merchants, this includes an examination of the merchant's entire site including links the merchant intends to display. We also investigate the website domain ownership and navigate through the checkout process in order to more fully understand the merchant's activities.

Chase Paymentech also participates in the MATCH program, which is hosted by MasterCard. The MATCH database lists merchants who have been terminated by other acquiring banks and serves as a reference tool to help protect payment processors like Chase Paymentech from entering into business with merchants that have known problems. In addition to engaging in a thorough review of merchant applicants, we proactively monitor our existing merchant base via a periodic review of the merchant itself. This procedure is similar to our initial due diligence and includes a subsequent review of the merchant's entire website.

We also make anonymous purchases at random merchant sites and at sites where something just does not look right. We also rely on transaction monitoring which is a continuous process that allows us to flag and review factors that are indicative of suspicious or unusual merchant activity. If we have any reason to believe that any suspicious activity has taken place, we file the appropriate suspicious activity reports with the authorities and investigate further.

In addition, we obtain information from MasterCard and Visa relating to suspicious merchant activity. In these circumstances we work with MasterCard and Visa to investigate and address the issue as quickly and thoroughly as possible. In the course of our processing payments for a large portfolio of merchants, we are aware of two legitimate merchants who have fallen prey to fraudulent and criminal activity to child pornographers. In both cases, those merchants unwittingly became conduits for child pornography related transactions.

I should note that in another circumstance a merchant was foolish enough to apply to us directly for payment services even though its website had links to child pornography. We discovered the child pornography during our review, reported the merchant to law enforcement, and denied the application. Although it is extremely rare for a child pornographer to gain access to our system, we remain extremely watchful and have an action plan we execute if such access occurs. For example, we immediately suspend our processing services for the merchant in question and visit the merchant's site to obtain as much information as possible to determine the scope and nature of the merchant's activities. We also notify NCMEC through a dedicated website. We notify the nearest office of the FBI and where appropriate we notify local law enforcement.

Any ultimate termination of the merchant account is also reported to the MATCH system maintained by MasterCard. In summary, Chase Paymentech strictly prohibits the use of its payment processing services in connection with child pornography. We have sophisticated and effective tools to prevent child pornographers from using our services and we constantly strive to stay one step ahead of the criminals. Chase Paymentech looks forward to working with the subcommittee as we coordinate our resources to eliminate the financial viability of child pornographers on the Internet.

[The prepared statement of William Matos follows:]

PREPARED STATEMENT OF WILLIAM MATOS, SENIOR DIRECTOR, CREDIT/RISK, CHASE  
PAYMENTECH SOLUTIONS, L.L.C.

Good morning Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee. My name is Bill Matos, and I am the Group Manager and Senior Director of Credit and Risk Management at Chase Paymentech Solutions, LLC. Chase Paymentech is strongly committed to combating child pornography, and it is my pleasure to appear before you today to discuss this important issue.

Chase Paymentech is one of the nation's largest processors of bankcard (*e.g.*, MasterCard or Visa) payment transactions for merchants. One of our primary roles is to contract with, and provide services to, merchants to enable them to accept MasterCard and Visa payment cards. The activities we perform in the bankcard systems are commonly referred to as "acquiring" or "payment processing" services. We provide these services for many types of electronic payment transactions, including those

conducted by credit card, debit card, gift card, electronic check, and other payment methods. We are headquartered in Dallas, Texas and have facilities in Florida, New Hampshire, and Arizona among other states.

### **In General**

Chase Paymentech has a strict prohibition against our services being used in connection with child pornography or any other illegal activity. Our credit and risk management team for our e-commerce merchant platform consists of 20 employees dedicated to screening potential merchants and monitoring our existing merchant base for a variety of risks, including those relating to child pornography. Our proactive efforts to screen and monitor our merchant base involve an extremely thorough and comprehensive process designed to ensure that our merchants are engaged in legal activities in compliance with our standards and those of MasterCard and Visa. In addition to the resources we dedicate to prevent the processing of child pornography-related transactions, Chase Paymentech has also coordinated with the National Center for Missing and Exploited Children (“NCMEC”), a variety of law enforcement agencies, and other companies to combat child pornography on the Internet.

### **Proactive Due Diligence**

Chase Paymentech has strict standards that must be met before we approve a merchant’s application for our services. We collect detailed information about merchant applicants and thoroughly review the application of each potential merchant to ensure the merchant meets our credit and risk management guidelines. This review process can take anywhere from two days for more well known merchants to five days for higher-risk merchants. Depending on the circumstances, we may collect the applicant’s financial statements and other financial information, tax returns, corporate documents, background information on the applicant’s ownership, detailed information relating to the applicant’s business and its history with respect to payment card acceptance, and other information required by the USA PATRIOT Act to properly understand who the merchant applicant is and to assess our credit and risk exposure as a result of processing the merchant’s transactions.

Not only do we assess the financial risks the merchant may pose to us as its payment processor, but we also engage in a thorough review of the compliance risks the merchant may present. Before we approve an applicant as one of our merchants, for example, we must understand the applicant’s business model and product line thoroughly. For on-line merchants, this includes a web site review by a member of our credit and risk management team who examines the merchant’s entire site, including links the merchant intends to display. We also investigate the web site domain ownership and navigate through the checkout process in order to understand more fully the merchant’s activities. If a merchant’s site is not live or fully functional at the time of application, approval is placed into a “funds hold” status which prevents the merchant from being funded for any transactions until such time as the live site can be thoroughly reviewed. Chase Paymentech also participates in the MATCH program, which is hosted by MasterCard. The MATCH database lists merchants who have been terminated by other acquiring banks and serves as a reference tool to help protect acquiring banks, like Chase Paymentech, from entering into business with merchants that are known problems.

It is our experience that child pornographers and others who engage in illegal activity rarely apply directly to us to obtain payment processing services. This is probably due in large part to the increasing sophistication of the criminals, their awareness of the due diligence we undertake as part of the application process, and their awareness of our on-going monitoring activities described below. For example, a sophisticated criminal enterprise is unlikely to subject itself to our review of its financial situation, its ownership, its lines of business, and its web site. This type of direct scrutiny

is a strong deterrent to child pornographers as well as other unqualified or unscrupulous applicants. If, nonetheless, we do uncover any activity or material that is illegal, we promptly report it to the appropriate law enforcement agency and offer our assistance in any law enforcement investigation.

#### **On-Going Monitoring**

In addition to engaging in a thorough initial review of applications, we also proactively monitor our existing merchants. In fact, there are three proactive means by which we monitor our Internet merchant base. The first method we use is a periodic review of the merchant itself. This procedure is similar to our initial due diligence and consists of a member of our risk management team reviewing the merchant's business including its entire web site. We engage in the review for several purposes, such as ensuring that the merchant has not established new lines of business or activities without notifying us, and ensuring that the merchant's practices have not evolved in a manner that creates a legal or compliance risk for us.

The second mechanism involves the use of anonymous visits and purchases from the merchant's web site, also known as "mystery shopping." We engage in mystery shopping based on random samplings of merchants. We also engage in mystery shopping if we believe there are unusual transaction patterns or if "something just does not look right" with respect to the merchant's transactions based on the merchant's profile. We then assess whether the transaction pattern suggests a more significant problem and further investigation is warranted. The use of mystery shopping allows us to verify the products that are actually delivered to the consumer, and to make sure that the web site transaction process is not simply a "cover" for unscrupulous activities.

The third tool in our on-going review of merchants is transaction monitoring. Transaction monitoring is a continuous process that allows us the opportunity to flag and review factors that are indicative of suspicious or unusual activity on the part of a merchant. Our monitoring of transactions can take a variety of forms. For example, we monitor the volume of transactions for each merchant as well as the merchant's average transaction amount to ensure that those parameters are consistent with that merchant's general business profile and comport with the parameters that were established upon our initial approval of the merchant. Any material discrepancy with respect to those parameters may suggest that the merchant is not engaged in the activities it once was or that the merchant is impermissibly processing transactions for another entity. Such unusual patterns would be a red flag indicating that the merchant should be examined more closely to ensure that it is still operating in a legitimate manner. If we have any reason to believe that any suspicious activity has taken place, we file the appropriate Suspicious Activity Reports with the authorities and investigate further. We also have the ability to suspend payment processing for that merchant.

In addition to our proactive efforts, we also obtain information from MasterCard and/or Visa relating to unusual activity that may be indicative of suspicious merchant behavior. For example, a bankcard association can analyze transaction activity involving a variety of card issuers and merchant acquirers to detect patterns that an acquirer alone may not be able to detect. MasterCard and Visa can also monitor the Internet for misuse of their brands by merchants, which is then relayed back to us and others whose merchant business may be affected. In these circumstances we work in concert with MasterCard and/or Visa to investigate and address the issue as quickly and thoroughly as possible.

#### **Response to Child Pornography**

As I described above, Chase Paymentech currently provides payment processing services for a large portfolio of merchants. In the course of our processing payments for that portfolio, we are aware of two legitimate merchants who have fallen prey to fraudulent and criminal activity by child pornographers. In both cases, those merchants

unwittingly became conduits for child pornography-related transactions that the merchants, in turn, submitted to us for processing. (I should note that in another circumstance, a merchant was foolish enough to apply to us directly for payment services, even though its web site had links to child pornography. We discovered the child pornography, reported the merchant to law enforcement, and denied the application.) Although it is extremely rare for a child pornographer to gain access to our system, we remain extremely vigilant and have an action plan we execute if such access occurs. If we become aware of facts suggesting that someone is attempting to process child pornography-related transactions through us, such as by doing so through another merchant, we immediately suspend our processing services for the merchant in question. It is important to understand that ceasing payment processing is a delicate issue, as it could "tip off" the criminals, in which case they would likely disappear without a trace. We therefore work closely with law enforcement authorities and, in addition to our efforts to stop payment processing, we immediately engage in other remedial action. For example, we visit the merchant's web site and engage in other research to obtain as much information as possible to determine the scope and nature of the merchant's activities. We also notify NCMEC through a dedicated web site, we notify the nearest office of the Federal Bureau of Investigation, and, where appropriate, we notify local law enforcement. Any ultimate termination of the merchant account is also reported to the MATCH system maintained by MasterCard.

#### **Conclusion**

Chase Paymentech strictly prohibits the use of its payment processing services in connection with child pornography. We have sophisticated and effective mechanisms to prevent child pornographers from using our services, and we have been successful in our efforts to combat child pornography on the Internet. Chase Paymentech looks forward to working with the Subcommittee as we coordinate our resources to eliminate the financial viability of child pornographers on the Internet. It has been my pleasure to describe our efforts to thwart payments for child pornography, and I would be happy to answer any questions you may have.

MR. WHITFIELD. Thank you very much. Ms. Mowder, you are recognized for 5 minutes.

MS. MOWDER. Chairman Whitfield, and members of the committee, my name is Kim Mowder, and I am the head of Risk and Fulfillment for BA Merchant Services, a subsidiary of Bank of America. BA Merchant Services provides card processing services across the United States. We applaud the committee's focus on this issue, and the coalition that Ernie Allen so ably chairs. We are proud to be a part of the collective effort and equally proud to be associated with the National Center for Missing and Exploited Children. I would like to begin my testimony by emphasizing that Bank of America's policy and practice is to vigorously screen for and avoid signing merchants that are engaged in any kind of questionable activity, let alone child pornography, and to terminate any relationships that subsequently change in that direction should that happen.

We simply have zero tolerance when it comes to issues like child pornography, and we are closely aligned with and cooperate with law enforcement at every level in their efforts to combat this issue. Bank of

America is the second largest acquirer of merchants credit card processing in America. We have been processing credit cards for merchants since 1958, and have approximately 700,000 active merchants in our portfolio. We take great pride in our very conservative risk averse approach to the merchant services business and do not hesitate to decline nearly 2,000 applications a year because the activity of the merchant is inconsistent with our policies.

Our underwriting policy clearly defines those merchant types whom we deem to be unacceptable for a card servicing relationship, and we are much more conservative than required by law. The business types routinely declined by us include adult entertainment products and services, dating and escort services, debt collection firms, pornography products and services, tobacco products being sold via mail order, telephone order or Internet sales, wire transfer of money, and any money service businesses including payday loans and check cashing. No exceptions are made on these businesses entities, and, again, we have zero tolerance for issues like child pornography.

Our process begins with the salesperson talking directly to a merchant, often face-to-face. Together they complete a merchant application that is then sent to our underwriting experts in our processing center. Our process is based on the principle of know your customer; not only to screen out undesirable activities, but also for potential business opportunities. Merchant applications contain profile information on the merchant's business including a description of the products and/or services being sold, how those sales occur, and demand deposit banking information. In addition, the merchant application may include personal name, address, and social security number information of the owner or officer of the business.

Underwriters reviewing new merchant applications validate the merchant's physical business address, confirmation of the products or services being sold, and the methods of sale. They also examine all pages and links in a merchant's website if there is one. All validations are documented should later comparisons become necessary. I have listed in my written testimony nine of the tools we use to properly evaluate merchant applications, including verifying physical inventory and contacting neighboring businesses. Based upon information received from these sources, the underwriter may find it necessary to perform additional due diligence, and should the merchant be selling products or services via the Internet, the merchant's Internet site is reviewed in depth, with substantial focus on embedded links to any other sites.

This identifies merchants that might be assisting other parties in sale of products or services that are unacceptable under our policies.

Screening for unacceptable activities does not end without additional due diligence process. The BA Merchant Services Risk Department performs daily monitoring of merchant transaction histories on existing merchant accounts. Investigators use an in house merchant transaction tracking tool designed to closely monitor daily processing activity, and based upon parameters preset at the time of approval, daily activity reports are generated on those merchants that appear to be processing sales transactions contrary to the expected norm based on the original terms of their processing agreement and the business size and type.

Risk investigators utilize the same due diligence previously described for new applicants to examine merchants appearing on any exception reporting in an effort to ascertain the merchant's current processing behavior. Should the investigation determine that the merchant subsequently has been engaging in unacceptable activities immediate actions are taken. We may terminate the merchant. The profile information is forwarded to the bank's investigation services, and the bank coordinates with law enforcement at that time. We, of course, work in close partnership with the card associations. They employ on our behalf a vast array of protocols designed to be a formidable line of defense and capture real time potential illegal activities.

Our efforts and theirs are not discrete but a seamless and cooperative venture to ensure we all prevent the use of our payment networks for such purposes. It is a partnership, made stronger by the coalition Ernie chairs. We have seen this work first hand. Although we are aware of only one instance in our nearly 5 decades of experience with our 700,000 active merchants, in 2005 MasterCard did alert us to the potential for child pornography being offered through a link that appeared on a merchant's website that was opened for the sale of software. The merchant filed a police report to substantiate that they knew nothing about the link, and we do not know if the site was pirated from overseas or whether the merchant changed it after the account was opened.

For our purposes, that did not matter. We immediately closed the account, consistent with our zero tolerance policy. But this does demonstrate the effectiveness of the partnerships between the acquirers and the associations, in addition to the due diligence we perform in combating these types of activities. This single instance also highlights another point I would like to make. The merchant, in question, even though they may have been victimized, was acquired by an independent sales organization and approved through a subsidiary that became affiliated with the bank in 2004. We have announced the divestiture of this company and are bringing all merchant acquiring in-house. We believe this strengthens our ability to vet, sign, and re-verify merchant activity to ensure it is consistent with our policy.



In summary, Bank of America has a zero tolerance policy for anything related to child pornography. We believe strongly that our investigations and due diligence procedures provide assurance that child pornography is not being processed through our service and we work closely with the card associations to close any merchants they identify as posing a risk. Finally, we support the collective efforts of the coalition to ensure that the legitimate electronic payments industry is neither wittingly or unwittingly facilitating the sale of online child pornography.

[The prepared statement of Kim Mowder follows:]

PREPARED STATEMENT OF KIM MOWDER, SENIOR VICE PRESIDENT, BANK OF AMERICA

Chairman Whitfield, Congressman Stupak and members of the committee, my name is Kim Mowder, and I am the Head of Risk and Fulfillment for BA Merchant Services, a subsidiary of Bank of America. BA Merchant Services provides card processing services for approximately 700,000 merchants across the United States.

First, like my colleagues, we applaud the Committee's focus on this issue and the coalition that Ernie Allen so ably chairs. We are proud to be a part of this collective effort. We are equally proud to be associated with the National Center for Missing and Exploited Children. We subscribe to and whole heartedly agree with all the benefits and progress Mr. Allen has described for you.

I would like to begin my testimony by emphasizing that Bank of America's policy and practice is to vigorously screen for and avoid signing merchants that are engaged in any kind of questionable activity, let alone child pornography, and to terminate any relationships that subsequently change in that direction, should that happen. We simply have zero tolerance when it comes to issues like child pornography. And like our colleagues, we are closely aligned with and cooperative with law enforcement at every level in their efforts to combat this issue.

Bank of America is the second largest acquirer of merchant credit card processing in America. We have been processing credit cards for merchants since 1958 and have approximately 700,000 active merchants in our portfolio. We take great pride in our very conservative, risk averse approach to the merchant services business and do not hesitate to decline nearly 2,000 applications a year because the activity of the merchant is inconsistent with our policies.

In that regard, our underwriting policy clearly defines those merchant types whom we deem to be "unacceptable" for a card servicing relationship. We are much more conservative than what is legally permissible. The following business types are routinely declined by us:

- Adult entertainment products/services
- Dating/escort services
- Debt collection firms
- Pornography products/services
- Tobacco products being sold via mail order, telephone order or Internet sales
- Wire transfer of money or any money service businesses (MSB) including payday loans and check cashing

No exceptions are made on these businesses entities and, again, we have zero tolerance for issues like child pornography.

Our process of thoroughly vetting merchant applications begins with a sales person talking directly to a merchant, often face-to-face. Together they complete a merchant application package that is then sent to the underwriting experts in our processing center.

Our process is based on the principle of “know your customer,” not only to screen out undesirable activities but also to look for other potential business opportunities.

Merchant application packages contain profile information on the merchant’s business that includes, but is not limited to, a description of products and/ or services being sold, a description of how sales will occur, and demand deposit banking information. In addition, the merchant application may include personal name, address and social security number information on the owner/officer of the business if it is a small or new business. This information is used in the due diligence process to validate the business type and ownership.

Underwriters reviewing new merchant application packages are charged with validating the merchant’s physical business address, confirmation of the products or services being sold, and the methods of sale (retail store front, mail order, Internet, etc.). All verifications are documented should later comparisons become necessary.

And, of course, all pages and links in a merchant’s web site are examined, copied and maintained for future comparisons.

We believe that validation of ownership, business address and type is a simple but critical part of this process and we use sources of information like the following to verify all application information:

- Local, state and federal record sites (county clerk, secretary of state, etc.)
- Multiple search engines (yellow pages, phone number search, reverse information look- up services)
- Telephone contact with nearby businesses to secure knowledge of merchant activity
- Calls to trade associations familiar with the merchant or merchant business type
- Better Business Bureau Reports
- Dun & Bradstreet Business Reports
- Marketing materials requested from the merchant
- Invoices for store inventory confirming products in inventory
- Invoices for previous sales (calls frequently made to buyers to confirm products purchased)

Based upon information received from the above sources, the underwriter may find it necessary to perform additional due diligence to arrive at a sound business decision. We will do whatever is necessary to ensure we are signing merchants consistent with our policies.

Again, should the merchant be selling products or services via the Internet, the merchant’s Internet site is reviewed in depth, with substantial focus on embedded links to any other sites to identify products/services offered for sale through links in the merchant’s site. This identifies merchants that may be assisting other parties in sale of products or services that are unacceptable under our policies. The underwriter copies all internet pages that have been reviewed and stores them in the merchant file, primarily so they can be periodically checked for subsequent deviations.

Screening for unacceptable activities does not end with the initial due diligence process. BA Merchant Services’ Risk Department performs daily monitoring of merchant transaction histories on existing merchant accounts. Investigators use an in house merchant transaction tracking tool with features that are designed to ensure close monitoring of merchant’s daily processing activity. Based upon parameters preset at the time of approval, daily activity reports are generated on those merchants that appear to be processing sales transactions that are contrary to the expected norm based on the original terms of their processing agreement and the business size and type.

Risk investigators utilize the same due diligence tools to investigate merchants appearing on any exception reporting as those used by the underwriters on new merchant

applications, all in an effort to gain an understanding of merchant's current processing behavior. Due diligence may include but not be limited to talking directly to cardholders to confirm transaction validity and makeup, communicating with the merchant's banking representative and speaking directly with the merchant to gain answers to specific questions. From their investigation, the investigator will determine what, if any, post due diligence action is required by our policies.

The risk investigator may elect to terminate the merchant account based upon the risk associated with the new information obtained in the investigation, establish a loss reserve fund to compensate for any elevated risk associated with the merchant's new method of operation, or take no action at all, if new information learned falls into acceptable parameters for the business type.

Should the investigation determine that the merchant subsequently has begun engaging in unacceptable activities, the following actions are taken immediately:

1. Merchant processing capability is terminated immediately;
2. Merchant profile information is forwarded to Bank of America's Investigative Services Division for immediate investigation; and
3. The bank coordinates with law enforcement.

And, of course, we work in close partnership with the Card Associations. They employ on our behalf a vast array of protocols, all designed to be a formidable line of defense and capture real time potential illegal activities. Our efforts and their efforts are not discrete but a seamless and cooperative venture to ensure we all prevent the use of our payment networks for such purposes. It is a partnership, made stronger by the coalition Ernie chairs.

We have seen this work first hand. Although we are aware of only one instance in our nearly five decades of experience and with our 700,000 merchants, in 2005 MasterCard did alert us to the potential for child pornography being offered through a link that subsequently appeared on a merchant's web site, a merchant account that was opened for the sale of software. The merchant filed a police report to substantiate they knew nothing about the link and we do not know if the site was pirated from overseas or whether the merchant added it after the account was opened. For our purposes, it did not matter. We immediately closed the account, consistent with our zero tolerance policy. But this does demonstrate the effectiveness of the partnerships between acquirers and the associations, in addition to the due diligence we perform in combating these types of activities.

This single instance also highlights another point I would like to make. The merchant in question, even though they may have been victims, was acquired by a sales organization subsidiary that became affiliated with the bank in 2004. We have announced the divestiture of this company and are bringing all merchant acquiring in-house. We believe this strengthens our ability to vet, sign and re-verify merchant activity to ensure it is consistent with our policy.

In summary, Bank of America has a zero tolerance for anything related to child pornography. We believe strongly that our investigations and due diligence procedures provide assurance that no undesirable merchant activities are being processed through our service and we work closely with Card Associations to close any merchants they identify as posing a risk. Finally, we support the collective efforts of the coalition and of this committee to ensure the legitimate electronic payments industry is neither wittingly or unwitting facilitating the sale of online child pornography.

MR. WHITFIELD. Thank you very much. Mr. Shalom, you are recognized for 5 minutes.

MR. SHALOM. Thank you. Good afternoon, Mr. Chairman, and members of the committee. My name is Ralph Shalom, and I am Associate General Counsel at First Data Corporation. I am pleased to be here today to discuss First Data's role in the payments industry, specifically merchant processing, as the committee continues its hearings into Internet child pornography. Let me begin my testimony by describing First Data, and the unique role we play helping millions of consumers, businesses, and governmental entities buy products and services on a daily basis. Many of you do business with First Data every day whether using an ATM/debit card to pay at a gas station, writing a check for groceries, buying a book online. There is a good chance that First Data is moving that transaction, at least part of the way, between the merchant and the consumer.

Although we have many interesting products and services that provide some type of payment processing, I will focus my testimony on merchant processing. Our merchant services business segment facilitates the ability of merchants to accept consumer transactions at the point of sale, whether the merchant operates a physical store, brick and mortar, or whether the merchant has a virtual or online presence. Our services enable businesses of all sizes to accept various forms of payments from consumers, including credit and debit cards. Together with the various financial institutions with which we work, we provide merchant processing services for 3.5 million merchants in the United States.

When we sign up or acquire merchants for processing services, we make great efforts to understand, one, who are our clients, and, two, what type of products or services do they sell. The answers to these questions not only drive technical aspects of how the accounts are set up, but they also inform us of the risk that the merchant might present to us, and, indeed, whether we are willing to accept the merchant at all. When merchants apply for services, they are asked questions to help us understand who they are, including providing taxpayer ID numbers, Social Security numbers, and other information. If the sale is made face-to-face the sales representatives are trained to make notations about the physical aspects of the merchant operations.

If the merchant is an online vendor, we require the merchant to provide us with the website address, which is then reviewed by our credit department. There are many businesses that we simply refuse to accept under our credit policies in which we operate. None of these policies allow for adult online video content. Merchant whose businesses are involved in what we understand to be illegal dealings, including the sexual exploitation of children, are automatically excluded. Several years ago we also made the determination to avoid businesses providing sexually oriented online video. When a merchant applies for an account

with us as part of the initial underwriting reviews, we pull a credit report, review the materials provided with the application, check the industry High Risk files, which you have heard about today as the MATCH file, and check the website if the business is described as being online.

We would disqualify a merchant from receiving an account if the merchant is involved in online gambling, online cigarette sales, online firearms sales, and certainly they are involved in sexually oriented online video content to name a few reasons. Merchants don't always tell us the truth when they describe what they are going to sell. Even if they have provided a processor like us with a website that describes their business, a merchant can operate another website that presents a different business proposition to the consumer. There is nothing in the credit card transaction record itself that would prevent a merchant from taking transactions and paying on one website and submitting them through an account that, in our records, we have associated with a legitimate website. Also, sometimes legitimate merchants will get co-opted into running transactions for another business.

As a result, our review of merchant activity continues beyond the initial underwriting. We review transaction activity for our merchants to determine if their processing has materially changed in ways that suggest the merchant is not who they claimed to be. Further, we continually evaluate new software and technology solutions to help us identify when a merchant has associated itself with illegal activity. Equally important, we maintain a liaison with law enforcement so that we can be notified when they are targeting specific merchants for illegal behavior.

From a merchant processing perspective, we see the financial piece of the transaction, which for most transactions is primarily the date, time, amount of sale, and card number. We don't know what the cardholder saw or what the cardholder was told when they were presented with the bank account information to complete the sale, nor do we know what the merchant presented to the cardholder to generate that sale. With billions of transactions running through our systems, individual transactions cannot be investigated. However, we do review merchant deposits for patterns that, in our experience, suggest the merchant may be of a different type than we originally understood.

For example, we might look at significant increases in transaction volume, in excess of what might be expected as normal growth, patterns of transaction amounts larger than would be expected for a business of the type described, abnormally high transactions which are questioned by cardholders or charged back, among other criteria. We process more than 100 pattern filters to identify patterns which suggest merchants that require additional review. We have a fraud department that is tasked with reviewing accounts that have tripped some of our suspicious activity

patterns to determine whether there is anything that suggests we can or should stop providing processing services.

As a result of the work of this department, we have terminated nearly 4,000 merchant accounts in the past 5 years. In preparation for this hearing, I have surveyed our managers in these areas and it appears that we have not seen incidents of child pornography in these reviews. However, we have identified instances where merchants submitted transactions for others, or we have found that some merchants were involved in sexually explicit materials against our credit policy. In these cases, we immediately shut down the merchant's accounts. It may very well be that some of these accounts that we shut down could have carried transactions originating in other types of material.

Let me be clear. We take this issue very seriously and we have cooperated extensively with law enforcement. For instance, we have kept accounts open at the request of law enforcement for limited times when we have been told that it is necessary to facilitate ongoing investigations. We have provided information and access to funds which resulted in criminal convictions and significant seizures of funds associated with criminal activity. At First Data, we have no tolerance for the sexual exploitation of children. Although identifying online merchants engaged in child pornography can be challenging, we are committed to taking additional steps to identify these entities and preventing them from using our systems to fund their illicit activities.

First, we are participating in a pilot project with MasterCard to identify illegal or unacceptable merchant activity by searching the Internet for Web pages that engage in sexual exploitation of children. Second, we participate in Financial Coalition Against Child Pornography. Two of the key components of the coalition are the creation of a clearinghouse, which will facilitate the sharing of information among the payments industry. We believe that this will be a valuable tool to help eradicate such illicit activity from the payment system. In addition, the coalition's efforts determine the best way to perform test transactions on targeted websites will help us more quickly and accurately identify who is processing particular payment transactions, so that we can work effectively with law enforcement to shut them down.

First Data takes seriously its role in protecting the payment system from activities that are illegal or against our policies and the card association rules. We provide effective, front-end diligence procedures to help us identify unqualified merchants, and we impose checks on existing merchants when they trip any of our existing suspicious activity patterns. The measures being undertaken by the Financial Coalition Against Child Pornography will help all of us in the payment system

identify and deter the funding for the online exploitation of children.  
Thank you.

[The prepared statement of Ralph Shalom, Esq. follows:]

PREPARED STATEMENT OF RALPH SHALOM, ESQ., ASSOCIATE GENERAL COUNSEL FOR  
LITIGATION, FIRST DATA CORPORATION

Good morning, Mr. Chairman and members of the Committee. My name is Ralph Shalom, and I am Associate General Counsel at First Data Corporation. I am pleased to be here today to discuss First Data's role in the payments industry, specifically merchant processing, as the Committee continues its hearings into Internet child pornography.

Let me begin my testimony by describing First Data, and the unique role we play helping millions of consumers, businesses, and governmental entities buy products and services on a daily basis. Most people don't realize it, but First Data's products and services touch people's lives every day. We make buying and selling easier. It is that simple. Many of you do business with First Data everyday - whether you are using an ATM/debit card to pay for gas at the gas station, writing a check to pay for groceries, buying a book online, getting cash from an ATM, paying for dinner with a credit card or using a gift card - there is a good chance that First Data is moving that transaction at least part of the way between the merchant and the consumer.

Although we have many interesting products and services that provide some type of payment processing, I will focus my testimony on merchant processing. Our merchant services business segment facilitates the ability of merchants to accept consumer transactions at the point of sale, whether the merchant operates a physical store (brick and mortar) or whether the merchant has a virtual - or online - presence. Our services enable businesses of all sizes to accept various forms of payments from consumers, including credit and debit cards. The term "processing" can be described as those functions associated with authorizing, capturing, and settling merchants' credit, debit, stored value and loyalty card transactions. We provide merchant processing services for some 3.5 million merchants in the U.S.

At First Data, a majority of these services are offered through alliance relationships with financial institutions. These arrangements are established as either revenue sharing alliances or equity alliances. We have revenue sharing alliances with financial institutions like SunTrust, CitiGroup, and Huntington Bank. We have equity alliances with major financial institutions like Wells Fargo, PNC, and JPMorgan Chase. Our equity alliances are run as independent companies and compete against one another and against our Revenue Sharing Alliances in the market place.

**Understanding How New Merchants Are Acquired**

When we sign up, or acquire, merchants for processing services, we make great efforts to understand (1) who are our clients and (2) what type of products or services do they sell? The answers to these questions not only drive certain technical aspects of how the accounts are set up, but these questions also inform us of the risk that the merchant might present to us and, indeed, whether we are willing to accept the merchant at all. When merchants apply for services, they are asked questions to help us understand who they are, including obtaining their taxpayer identification number or their Social Security number. If the sale is made face-to-face, sales representatives are trained to make notations about the physical aspects of the merchant. If the merchant is an online vendor, we require the merchant to provide us with its Web site address which is then reviewed by our credit department.

There are many businesses that we simply refuse to accept under the credit policies in which we operate. Each of the alliances has its own credit policy that was developed

jointly with First Data. None of these policies allow for adult online video content. Merchants whose businesses are involved in what we understand to be illegal dealings, including the sexual exploitation of children, are automatically excluded. Several years ago we also made the determination to avoid businesses providing sexually oriented online video content. When a merchant applies for an account with us, as part of the initial underwriting reviews, we pull a credit report, review the materials provided with the application, check the industry High Risk files, and check the Web site if the business is described as being online. We might disqualify a merchant from receiving an account from us if the merchant is involved in online gambling, online cigarette sales, online firearms sales, or if they are involved in sexually oriented online video content, to name a few reasons. In addition, we conduct additional policing on non face-to-face prescription drug sellers.

**Understanding How Merchants Are Monitored for Fraud or Other Illegal or Unacceptable Practices**

Merchants don't always tell us the truth when they describe what they are going to sell. Even if they have provided a processor like us with a Web site that describes their business, a merchant can easily operate other Web sites that present a different business proposition to the consumer. There is nothing in the credit card transaction record that would prevent a merchant from taking transactions obtained on one Web site and submitting them through an account that, in our records, we have associated with a legitimate Web site. Also, sometimes legitimate merchants will get co-opted into running transactions for another business.

As a result, our review of merchant activity continues beyond the initial underwriting of the account. We review the transaction activity for our merchants to determine if their processing materially changes in ways that suggest the merchant is not who they claimed to be. Further, we continually evaluate new software and technology solutions to help us identify when a merchant has associated itself with illegal activity. Equally important, we maintain a liaison with law enforcement so that we can be notified when they are targeting specific merchants for illegal behavior.

From a merchant processing perspective, we see the financial piece of the transaction, which for most transactions is simply the date, time, amount of sale and card number, as well as industry specific criteria necessary for assisting bank card issuers in making authorization decisions and for qualifying a transaction through the card associations (e.g. VISA and MasterCard) to obtain certain interchange rates. In other words, we don't know what the cardholder saw or what the cardholder was told when he or she presented their bank card account information to complete the sale. Nor do we know what the merchant presented to the cardholder that generated the sale.

With billions of transactions running through our systems, individual transactions cannot be investigated. However, we do review merchant deposits for patterns that, in our experience, suggest the merchant may be of a different type than we originally understood. For example, we might look at significant increases in transaction volume, in excess of what we might expect as normal growth; patterns of transaction amounts larger than would be expected for the type of business described; an abnormally high number of transactions which are questioned by the cardholders or charged back; among others. We also run bank card transactions through more than 100 pattern filters to identify which merchants merit an additional review.

We have a fraud prevention department that is tasked with reviewing accounts that have tripped some of our suspicious activity patterns to determine whether there is anything that suggests we can or should stop providing processing services. As a result of the work of this department, we have terminated nearly 4,000 merchant accounts in the past five years. In preparation for this hearing, I have surveyed our managers in these areas and it appears that we have not seen incidents of child pornography in these



reviews. However, we have identified instances where merchants submitted transactions for others, or we have found that some merchants were involved in sexually explicit materials. In these cases, we immediately shut down the merchant's accounts. It may very well be that some of these accounts that we shut down could have carried transactions originating with sexually explicit material.

Let me be very clear: We take this issue very seriously and have cooperated extensively with law enforcement. For instance, we have kept accounts open for a limited time when we have been told that is necessary to facilitate an ongoing investigation and have provided information and access to funds which have resulted in criminal convictions and significant seizures of funds associated with criminal activity.

#### **First Data Participates in the Financial Coalition Against Child Pornography**

At First Data, we have no tolerance for the sexual exploitation of children. Although identifying online merchants engaged in child pornography can be challenging, we are committed to taking additional steps to help identify these entities and prevent them from using our systems to fund their illicit activities. First, we are participating in a pilot project with MasterCard to identify illegal or unacceptable merchant activity by searching the Internet for Web sites that engage in the sexual exploitation of children. Second, we participate in the Financial Coalition Against Child Pornography. As you know, the goals of the Coalition are to: (1) establish a global clearinghouse on child pornography; (2) create a proactive system to enable the financial services industry to deal with illegal uses of its systems to disseminate child pornography; (3) create a system for reporting suspected child pornography; and (4) implement monitoring and due diligence checks. Two of the key components of the Coalition are the creation of the clearinghouse, which will facilitate the sharing of information among the payments industry. We believe this will be a valuable tool to help eradicate such illicit activity from the payments system. In addition, the Coalition's efforts to determine the best way to perform test transactions on targeted Web sites will help us more quickly and accurately identify who is processing those particular payment transactions, so that we can work effectively with law enforcement to shut them down.

#### **Conclusion**

In summary, First Data takes seriously its role in protecting the payments system from activities that are illegal or against our policies and the card association rules. We employ effective, front-end due diligence procedures to help us identify unqualified merchants, and we impose checks on existing merchants when they trip any one of our existing suspicious activity patterns. Finally, the measures being undertaken by the Financial Coalition Against Child Pornography will help all of us in the payments system identify and deter the funding for the online exploitation of children.

Thank you.

MR. WHITFIELD. Thank you, Mr. Shalom. Mr. Strider, you are recognized for 5 minutes.

MR. STRIDER. Good afternoon, Mr. Chairman, and members of the subcommittee. On behalf of NOVA, I would like to thank you for the opportunity to address NOVA's efforts as a member of the financial services industry, to combat the sale and distribution of child pornography over the Internet. Specifically, I would like to provide the subcommittee with an overview of the due diligence NOVA conducts before approving a new merchant and the ongoing monitoring NOVA performs on existing merchants, and the actions that NOVA takes if a

merchant is subsequently engaged in prohibited or illegal activity, which would include child pornography.

Nova is committed to preventing merchants engaged in child pornography from using its payment services. In addition to NOVA's individual efforts, which I will describe during my testimony, NOVA has joined forces with others in the financial services community such as the FCACP. By way of background, NOVA provides integrated credit and debit payment processing, e-check, gift card and prepaid solutions, and software applications to businesses. Established in 1991, NOVA is currently the third largest acquirer of credit card transactions in the United States with approximately 800,000 merchants nationwide. Since its acquisition by U.S. Bancorp in 2001, NOVA has been a wholly-owned subsidiary of U.S. Bank National Association, the sixth largest financial institution in the U.S.

NOVA is somewhat unique in the acquiring industry since it is a wholly-owned subsidiary of a national banking organization. This means that in addition to being subject to the rules and regulations of the card associations, NOVA is also regulated and routinely audited by the Office of the Comptroller of the Currency and the Federal Reserve. The regulators regularly review NOVA's sales and operations departments to ensure compliance with the policies and procedures of both NOVA and U.S. Bank. I would like to turn now to a brief review of NOVA's operational policies and procedures regarding the approval of new merchants, the monitoring of existing accounts, and the steps NOVA would take in the event a merchant was suspected of being engaged in child pornography. It is important to note Nova applies these policies and procedures to every prospective and approved merchant account serviced by NOVA.

First and foremost, NOVA has a strict policy against processing for a merchant engaged in any illegal activity including child pornography. Moreover, NOVA's credit and underwriting policy strictly prohibits the approval of any adult business regardless of the legality of such activity. NOVA strives to prevent any such business from being approved by employing a very strict credit and underwriting policy, and undertaking a rigorous due diligence review of every prospective merchant account.

NOVA also conducts a rigorous due diligence review of every prospective due diligence account. The due diligence process generally starts with a physical site survey of a brick and mortar merchant to confirm the existence of the merchant and the type of goods and services sold. Merchants engaged in business on the Internet for whom a physical site survey is not possible are classified as higher risk and subjected to additional scrutiny by NOVA's credit and underwriting unit. This additional scrutiny includes a full scan of the merchant's website as well

as all links to other websites, a search of the merchant's name on Lexis/Nexis, Google, and other search engines, cross-reference of the merchant name, address, and other information pertinent to that account, a credit report, a telephone interview that includes challenge questions to confirm the applicant and the merchant are one and the same.

Credit and background checks of the business and, in many instances, its principals or owners are also a regular part of NOVA's due diligence process. NOVA also queries the MATCH file to determine if the business or its principals, partners, or owners have been reported by a previous acquirer for violations of the card association rules. Additionally, NOVA's Anti-Money Laundering Policy requires NOVA to screen all prospective merchants against various sanctions including the list maintained by the Office of Foreign Asset Control.

In most cases, NOVA is able to confirm a prospective account is legitimate and creditworthy through the diligence process. From time to time, however, information discovered during the diligence process phase raises a red flag for NOVA leading to further investigation, and in certain cases there is a decline of an account. Red flags indicating a prospective account may not be legitimate include the use of false names, addresses, social security numbers, no refund policy posted on the website, products and services offered for sale other than those described in the application, and, with respect, to adult businesses specifically, links to adult websites and advertisements for things such as sex toys.

Once a merchant account is approved, NOVA continues to monitor the account for changes in processing parameters through automated systems that queue a merchant for further review if certain changes are noted.

[The prepared statement of David Strider follows:]

PREPARED STATEMENT OF DAVID STRIDER, EXECUTIVE VICE PRESIDENT, NORTH AMERICAN OPERATIONS, NOVA INFORMATION SYSTEMS, U.S. BANCORP

Good morning Mr. Chairman and Members of the Subcommittee. On behalf of NOVA, I would like to thank you for this opportunity to address NOVA's efforts, as a member of the financial services industry, to combat the sale and distribution of child pornography over the Internet. Specifically, I would like to provide the Subcommittee with an overview of the due diligence NOVA conducts before approving a new merchant account, the ongoing monitoring NOVA performs on existing merchant accounts and the actions NOVA takes if a merchant account is engaged in prohibited or illegal activity, which would include child pornography.

NOVA is committed to preventing merchants engaged in child pornography from using its payment services. In addition to NOVA's individual efforts, which I will describe during my testimony today, NOVA has joined forces with others in the financial services industry, the National Center for Missing & Exploited Children and the International Centre for Missing & Exploited Children as a member of the Financial Coalition Against Child Pornography. As you know, the goal of the FCACP is to eradicate commercial child pornography by 2008.

By way of background, NOVA provides integrated credit and debit payment processing, electronic check services, gift card and prepaid solutions, and software applications to businesses. Established in 1991, NOVA currently is the third largest acquirer of credit card transactions in the United States with approximately 800,000

merchants nationwide. Since its acquisition by U.S. Bancorp in 2001, NOVA has been a wholly-owned subsidiary of U.S. Bank National Association, the sixth largest financial institution in the United States.

NOVA is somewhat unique in the acquiring industry since it is a wholly-owned subsidiary of a national banking organization. This means that in addition to being subject to the rules and regulations of the card associations, NOVA is also regulated and routinely audited by the Office of the Comptroller of the Currency and the Federal Reserve. The regulators regularly review NOVA's sales and operations departments to ensure compliance with the policies and procedures of both NOVA and U.S. Bank.

I would like to turn now to a brief review of NOVA's operational policies and procedures regarding the approval of new merchant accounts, the monitoring of existing merchant accounts and the steps NOVA would take in the event a merchant account was suspected of being engaged in child pornography. It is important to note NOVA applies these policies and procedures to every prospective and approved merchant account serviced by NOVA.

First and foremost, NOVA has a strict policy against processing for a merchant engaged in any illegal activity including child pornography. Moreover, NOVA's credit and underwriting policy strictly prohibits the approval of any adult business regardless of the legality of such activity. NOVA strives to prevent any such business from being approved by employing a very strict credit and underwriting policy to, and undertaking a rigorous due diligence review of, every prospective merchant account.

NOVA also conducts a rigorous due diligence review of every prospective merchant account. The due diligence process generally starts with a physical site survey

of a “brick and mortar” merchant to confirm the existence of the merchant and the type of goods and services sold. Merchants engaged in business on the Internet, for whom a physical site survey is not possible, are classified as “higher risk” and are subjected to additional scrutiny by NOVA’s credit and underwriting department. This additional scrutiny includes a full scan of the merchant’s website as well as all links to other websites; a search of the merchant name on Lexis/Nexis, Google and other search engines; cross-reference of the merchant name, address and phone number against the credit report; and a telephone interview that includes challenge questions to confirm the applicant and the merchant are one and the same.

Credit and background checks of the business and, in many instances, its principals, partners or owners are also a regular part of NOVA’s due diligence process. NOVA also queries the card associations’ MATCH file (which stands for Member Alert to Control High Risk Merchants) to determine if the business or its principals, partners, or owners have been reported by a previous acquirer for violations of the card association rules and regulations. Additionally, NOVA’s Anti-Money Laundering Policy requires NOVA to screen all prospective merchants against various sanctions lists including the SDN list maintained by the Office of Foreign Asset Control.

In most cases, NOVA is able to confirm a prospective account is legitimate and creditworthy through the diligence process. From time to time, however, information discovered during the diligence phase raises a “red flag” for NOVA, leading to further investigation and, in certain cases, the decline of an account. Red flags indicating a prospective account may not be legitimate include the use of false names, addresses, social security numbers; no refund policy posted on the website; products and services

offered for sale other than those described in the application; and, with respect to adult businesses specifically, links to adult websites and advertisements for sex toys.

Once a merchant account is approved, NOVA continues to monitor the account for changes in processing parameters through automated systems that queue a merchant for further review if certain changes are noted in the system. The parameters reviewed in this fashion include the size of a merchant's average sale and the number and level of authorization requests, declines, sales, credits and chargebacks. Additionally, NOVA's loss prevention department routinely monitors merchant accounts for changes in type of business (for example, from a retail to a mail order/telephone order environment) and for changes in the types of product or services sold. For Internet merchants, these analysts verify there have been no changes through a number of avenues including a review of the merchant's website; review of links to other websites; and in some cases, test transactions or calls to cardholders to confirm the nature of goods and services being provided.

In addition to dedicating internal resources to these tasks, NOVA has engaged an industry-approved vendor to assist with the ongoing review of merchant websites. NOVA regularly provides this vendor with merchant websites to review. Given NOVA's policy against processing for any type of adult merchant, the vendor searches merchant websites for trigger words associated with adult businesses generally including "sedation" and "bestiality" as well as trigger words associated with child pornography such as "Lolita", "pedo" and "preteen."

Merchants confirmed to be engaged in activities prohibited under NOVA's policies are closed and reported to the MATCH file as appropriate under the card association rules and regulations. Many of these types of businesses, while prohibited

under NOVA's policy, are legal and consequently are not reported to law enforcement or to the MATCH file.

Merchants suspected of being engaged in an illegal activity, which of course is also prohibited under NOVA's policies, are reported to the appropriate law enforcement agency. NOVA frequently works with law enforcement in the subsequent investigation. In some cases law enforcement has required NOVA to keep a merchant account open to allow law enforcement to gather information about the merchant or the consumers purchasing from the merchant. Once the investigation is complete, and with the approval of the law enforcement agency, NOVA then closes the merchant account and reports the merchant and its owners to the MATCH file as required.

With that general overview, allow me to turn to the very few circumstances of suspected child pornography NOVA has encountered and then to the reasons why the number of instances has been so low. Over the last six years, NOVA has discovered or been notified of only a handful of instances of suspected child pornography. In each case, NOVA had approved the merchant's application for a different type of business. The suspicious activity was identified in some cases by NOVA and in others by the card associations or law enforcement.

NOVA investigated each incident thoroughly and worked closely with law enforcement and the card associations as requested. In many of the cases, the investigation revealed the merchant was engaged in an adult business but did not confirm the merchant was engaged in child pornography. Given its strict policy against any adult business, NOVA immediately closed those accounts and reported the merchant and its principals, partners, owners to MATCH if required under the card association regulations.



In one case in particular, law enforcement requested that NOVA keep the merchant account open to allow enforcement to complete its investigation. Following completion of the investigation, NOVA terminated the merchant account and reported the merchant and its principals, partners, owners to MATCH as required under the card association regulations.

NOVA firmly believes its experience, or lack thereof, with merchants peddling child pornography is the result of a number of factors including its stringent approval policy and diligence requirements and continued monitoring of its merchant accounts, and the fact that those policies and procedures apply across the board to every prospective merchant and approved merchant serviced by NOVA. That said, those engaged in illegal activity of any type constantly look for ways to beat the system. Therefore, NOVA and its colleagues must remain vigilant and keep abreast of changes in methods and technology in order to prevent those engaged in illegal activity from taking advantage of the payment system. NOVA fully supports the efforts of the FCACP to assist acquirers in that regard by providing a forum for sharing information and experiences from which everyone in the industry can learn.

I hope my comments today have been informative. I appreciate the Subcommittee's time and I look forward to answering any questions you may have.

MR. WHITFIELD. Mr. Strider, excuse me for interrupting you but time has expired, and we have votes on the floor, and I just missed one

vote. Because we have another series of votes, we could keep you here for quite a while, but I think what I am going to do is just ask a couple of brief questions that can be answered rather quickly, and we have your testimony which we appreciate your preparing very much.

I want to just ask a couple of questions, and then we are just going to adjourn this hearing but we may be back in touch with all of you as we move forward on some specific things that have come up. But I do thank you for your time and for testifying here today and for your patience.

Here is one of the questions. Over the last 4 years, I would just like to know, if you can answer this question, how many Internet merchants have you identified that were engaged in commercial child pornography? Mr. Matos, can you answer that question?

MR. MATOS. That would be two merchants that were actually engaged.

MR. WHITFIELD. Two. Okay. Ms. Mowder.

MS. MOWDER. One.

MR. WHITFIELD. One.

MR. SHALOM. We haven't identified any on our reviews that engaged in Internet child pornography. We have been advised by law enforcement by investigations they were conducting in one instance.

MR. WHITFIELD. Okay. Mr. Strider.

MR. STRIDER. Two, and two others were notified by law enforcement.

MR. WHITFIELD. Okay. Now one other question. When determining whether to sign up a merchant do, the Internet merchants receive any greater scrutiny than a brick and mortar merchant?

MR. MATOS. Absolutely, Mr. Chairman. Our present platform which would include Internet e-commerce based merchants, we consider those high risk transactions and those receive a much greater scrutiny than retail.

MR. WHITFIELD. Okay. Ms. Mowder.

MS. MOWDER. Yes, Mr. Chairman, very similar to my colleague.

MR. WHITFIELD. Okay.

MR. SHALOM. Our approach is consistent with that.

MR. STRIDER. It is the same.

MR. WHITFIELD. Okay. Well, you all have been great. Thank you so much for taking time to be with us. We look forward to working with you, and I would adjourn the hearing at this point.

[The information follows:]

Article 35

**THE WALL STREET JOURNAL**

**Dangerous Mix: Internet Transforms Child Porn Into Lucrative Criminal Trade --- Company in Belarus Collected Millions From Pedophiles; A Landmark Prosecution --- Agent's Rendezvous in Paris**

By Cassell Bryan-Low

2438 words

17 January 2006

The Wall Street Journal

A1

English

(Copyright (c) 2006, Dow Jones & Company, Inc.)

On a Saturday morning in October 2003, federal agents raided the apartment of Chicago pediatrician Howard Marc Watzman. They found two computers with more than 3,000 images of boys and girls as young as 4 years old being sexually exploited. Mr. Watzman was later sentenced to five years in prison for possessing child pornography.

The case is one of more than a thousand stemming from a broad international probe into a company called **Regpay** Co. in the former Soviet republic of Belarus. **Regpay** gathered lurid images and sold them to pedophiles around the world with the help of U.S. companies that collected credit-card payments.

**Regpay** offers a window into how the Internet has transformed what was once a cottage industry into a sophisticated business. The company is at the center of what U.S. law-enforcement officials call the largest Internet child-pornography investigation to date and the first to follow the international financial trail of child-porn sales. The probe has discovered the names of some 40,000 Americans who downloaded child porn and led to more than 1,400 arrests world-wide including about 330 in the U.S. At least three users arrested in the U.S. have committed suicide.

Some estimate the Internet child-pornography business could bring in billions of dollars annually. "It has now become a revenue generator for organized groups," says Ernest Allen, head of the National Center for Missing and Exploited Children, an Alexandria, Va., nonprofit.

U.S. and U.K. child-protection experts estimate that there are thousands of commercial Web sites containing child pornography and as many as 100 new ones pop up each month. They say the children being abused are becoming younger and include toddlers. The potential market is large: As many as one in 1,000 men has a sexual interest in children, estimates Hamish McCulloch, assistant director for trafficking in human beings at Interpol, the international police organization. The problem is less common in women, though not unknown.

In the 1980s, a broad crackdown in the U.S. and other countries largely choked off the flow of child pornography, forcing it out of its traditional niche of sex bookshops and into underground networks of collectors. When the Internet became widespread in the 1990s, it instantly proved popular with pedophiles. There was little risk of prosecution amid a lack of law-enforcement scrutiny.

Child-pornography Web sites draw "people who had never dreamed of indulging in the fantasy" by giving them the perception of anonymity, says Kevin Zuccato, director of the Australian federal police's high-tech crime center. Thanks to better Internet connections, **Regpay's** users were able to download millions of images in just one year, something that "simply wouldn't have been possible" 10 years ago, says Mr. Zuccato, whose team coordinated the arrests of **Regpay** customers in Australia.

The Internet emboldens consumers of child pornography to seek out increasingly graphic material. "I wanted to see more and more abusive pictures," says Chris, a technician for a leisure company, in a video interview used for training purposes by the Lucy Faithfull Foundation, a British child-protection charity.

In the video, Chris says he started off spending a few minutes a week searching for child porn on the Web. Soon he was spending as much time viewing images "as I humanly could," and he even recalls one 24-hour session. Chris served a three-year probationary sentence for possessing child pornography in a case unrelated to **Regpay**. The foundation made the video available on condition that his last name not be used.

At first it was mostly pedophiles themselves who distributed the images circulating on the Internet. But the industry's profit potential has increasingly attracted organized criminals who bring with them business and money-laundering skills.

**Regpay's** president was Yahor Zalatarou, a 27-year-old man with a talent for computers. The son of an engineer and a teacher, Mr. Zalatarou grew up in the Belarus capital of Minsk. He worked with Aliaksandr Boika, 31, who has a background in computer software, and Alexei Buchnev, 28, a translator. All three are now in jail.

U.S. law-enforcement agencies suspect that Mr. Zalatarou had connections to a larger criminal network and say their investigation is continuing. Robert Little, a New Jersey lawyer for Mr. Zalatarou, says there were "levels of hierarchy above him." Mr. Little adds that Mr. Zalatarou denies his bosses were "mafia-related."

The allegations against **Regpay** are detailed in indictments returned by a Newark, N.J., federal grand jury in December 2003 and October 2004.

At first the company was called Trustbill. It changed its name to **Regpay** after receiving two cease-and-desist notices from the Michigan attorney general's office in August and September 2002, according to an affidavit by Internal Revenue Service special agent Maria Reverendo attached to a July 2003 complaint against Messrs. Zalatarou and Boika.

**Regpay** processed payments for more than 50 third-party child-pornography sites, and ran at least five of its own with names like darkfeeling.com, lust-gallery.com and lolitties.com. "All girls are under 14," read the advertising blurb for the lolitties.com site, according to Ms. Reverendo's affidavit. Another site advertised "6,000 high-resolution professional images."

The majority of images of child pornography come from the U.S. or Western Europe, law-enforcement officials say. Abusers typically are family members or someone else known to the victim. The advent of digital cameras and camcorders has fueled an explosion in the material available online. Because pedophiles often are willing to share their images at little or no cost by uploading them to the Internet, it is easy for third parties like **Regpay** to obtain and package content on their own sites.

Lawyers for Messrs. Zalatarou, Boika and Buchnev say their clients weren't involved in making child pornography. Some U.S. law-enforcement officials suspect links between **Regpay** and the producers of some images on its Web sites because Belarus authorities said they found a studio used to make pornographic pictures in the same building as **Regpay's** offices in Minsk. But U.S. authorities say they haven't recovered any child pornography from that studio.

Subscribers paid up to \$75 per month to access **Regpay's** sites and the sites for which it handled payments, says Kevin O'Dowd, an assistant U.S. attorney in Newark and a lead prosecutor on the case. **Regpay** processed about \$8 million in payments from June 2002 to June 2003 and pocketed more than 75% of that, according to U.S. authorities. They believe Mr. Zalatarou personally earned only about \$20,000 to \$50,000 a month, bolstering suspicions that he was part of a larger enterprise.

The key to **Regpay's** business was getting money from the credit cards of subscribers in the U.S., Europe and elsewhere into its own accounts, at least one of which was in Latvia, a former Soviet republic neighboring Belarus. Credit-card payments from many customers went first to a small Fort Lauderdale, Fla., company called Connections USA Inc. Connections, which had a legal business in online and telephone dating services, had signed up as a merchant in credit-card networks. Both Visa and MasterCard cooperated in the investigation.

Connections forwarded subscriber payments to a **Regpay** account in Latvia, according to the indictments. The money was transferred from a Morgan Stanley account -- apparently the business account for

Connections -- to a Deutsche Bank AG account and from there to Aizkraukles Bank in Riga, Latvia, according to the IRS agent's affidavit.

Altogether Connections helped launder about \$3 million from June 2002 through June 2003 in return for a commission of more than 11% on the funds transferred, according to the indictments.

No banks have been charged in the **Regpay** case. Financial institutions have a duty under U.S. law to know their customers and file reports if they detect suspicious activity, but how much a bank should investigate "is still very much a judgment call," says Karen Petrou, managing partner of Federal Financial Analytics Inc., a research and consulting firm in Washington.

The three banks declined to comment on whether they reported suspicious activity in this case. Morgan Stanley spokesman Hugh Fraser says his institution "performed appropriate diligence on the account" and has been cooperating with law enforcement. A Deutsche Bank spokeswoman declined to comment.

Aizkraukles Bank said in a statement that laws prohibit it from talking about specific clients but that in 2003 it investigated several transactions related to the sale of child pornography online and reported its findings to authorities in Latvia.

Mr. O'Dowd, the assistant U.S. attorney in Newark, declined to comment on whether any bank was a target of investigation. In general, he says, banks "really need to focus on continuing due diligence" but "sometimes the ongoing due diligence isn't there."

**Regpay** also used another U.S. company, LB Systems Inc., run by a Belarussian man living in Los Angeles, to transfer funds to a **Regpay** account in Latvia, according to the indictments.

The U.S. investigation began in early 2003 when undercover federal agents in Newark and Washington began purchasing child pornography from Web sites in an attempt to track down people producing and profiting from the sites. It marked the first time the U.S. government followed the financial trail of online child pornography, according to U.S. Immigration and Customs Enforcement. The effort was conducted by the U.S. attorney's office in Newark in conjunction with IRS agents, postal inspectors and immigration officials.

Credit-card and other records led agents to Connections. In June 2003, federal agents searched Connections' offices and secured cooperation from the company's owner, Arthur P. Levinson. Mr. Levinson later pleaded guilty in Newark federal court to a criminal violation of structuring financial transactions to avoid reporting requirements. His lawyer, Henry Klingeman, says Mr. Levinson didn't know that **Regpay's** business involved child pornography.

Connections and two of its employees pleaded guilty to money laundering or failure to report the offense to law enforcement. Connections forfeited more than \$1.1 million and was dissolved. Mr. Levinson and the two employees await sentencing.

Posing as Mr. Levinson, federal agents began communicating with Mr. Zalatarou, the **Regpay** president, and others at the company via email and phone about payment arrangements. Because the U.S. doesn't have an extradition arrangement with Belarus, U.S. authorities couldn't ask the country to hand over Mr. Zalatarou and his cohorts. The federal agents lured Mr. Zalatarou to France under the pretense of discussing future business opportunities.

An agent met with Mr. Zalatarou and Mr. Buchnev, the translator, at the restaurant of the Hotel Concorde La Fayette in Paris on July 30, 2003. Following the meeting, French police arrested the two men in the hotel's lobby. Two days later, Interpol officers arrested Mr. Boika, the **Regpay** software expert, at a hotel on the northeast coast of Spain, where he was on vacation with his wife. Spain and France have since extradited the three men to the U.S.

Mr. Zalatarou and Mr. Boika both pleaded guilty in February 2005 to money laundering and conspiring to distribute or advertise child pornography. They are in jail in New Jersey awaiting sentencing and face up to 40 and 50 years in prison, respectively. In their native Belarus, penalties for those crimes range from a fine to five years in prison.

Mr. Zalatarou declined to be interviewed. Mr. Little, his lawyer, says he has "accepted his responsibility." Mr. Zalatarou left a wife, Anna, and a 3-year-old daughter behind in Minsk. Ms. Zalatarova, an English teacher, describes Mr. Zalatarou as an "ideal husband and wonderful father" who attended church regularly. She says she "cannot admit the possibility" that he was involved in child pornography.

Mr. Boika, who also has a wife and young child in Belarus, didn't respond to a letter mailed to him in jail. His lawyer in New Jersey, Richard Verde, says Mr. Boika "isn't a bad young man" and "is sorry for what he did."

Mr. Buchnev has pleaded guilty to conspiracy to distribute child pornography. He faces up to 20 years in prison. His lawyer, Maria Noto, says he didn't know **Regpay** was involved with child pornography until the July 2003 meeting in Paris with the undercover agent. He "regrets his involvement, as limited as it was," she says.

Federal agents seized server computers in Texas and Virginia that **Regpay** leased to run its business. The servers yielded credit-card transactions from about 90,000 customers. Almost half were in the U.S., with others as far away as Italy, Hong Kong and New Zealand.

The 330 **Regpay** subscribers arrested in the U.S. include teachers, priests and Boy Scout volunteers. Among them was Richard G. Fleischer, a 37-year-old divorced father of two who worked as a home-delivery manager for a newspaper in Florida. Police raided Mr. Fleischer's Tallahassee, Fla., home in August 2004 and found more than 1,100 images and video clips of child porn.

Mr. Fleischer told officers he knew he was "doing things I didn't need to do" but was "too scared to talk to anybody" about his problem and even cut off his Internet access to try to escape the temptation, police records show. He pleaded guilty in Florida federal court to possession of child pornography in December 2004 and is serving 15 years in prison.

Mr. Watzman, the pediatrician arrested in Chicago, spent an average of about \$1,000 a month purchasing child porn from more than 100 Web sites, according to court filings in his case. He couldn't be reached by phone and didn't respond to a letter mailed to his home. His lawyer, Thomas Durkin, says the 39-year-old Mr. Watzman, "like many people, became addicted to pornography." Mr. Watzman pleaded guilty but is appealing certain elements of his case.

Mr. O'Dowd, the **Regpay** case prosecutor, says the probe dealt a big blow to commercial distribution of child pornography on the Internet, "but it wasn't a kill shot." He says online distributors are switching from credit cards to electronic-currency systems, which leave less of a paper trail. Law-enforcement officials suspect the people to whom Mr. Zalatarou reported continue to operate under a different name.

**Dirty Trail**  
How some funds flowed from customers to Regpay, a child-pornography distributor, between June 2002 and June 2003:

- ① Customers paid up to \$75 a month by credit card.
- ② Connections USA, a Florida company, processed payments and kept 11% commission.
- ③ Funds flowed through accounts at Morgan Stanley, Deutsche Bank and Latvia's Alzraukles Bank to Regpay operators in Belarus.

Source: court filings



Yehor Zalatarou



Aliaksandr Boika

Document J000000020060117e21h0002J

More Like This

Related Factiva Intelligent Indexing™

+

© 2006 Dow Jones Reuters Business Interactive LLC (trading as Factiva). All rights reserved.  
UI 22.10.0 - Wednesday, June 21, 2006 8:15:06 AM

**Christian, Karen**

---

**From:** Andrews, Kelli  
**Sent:** Tuesday, June 06, 2006 3:17 PM  
**To:** Christian, Karen; Nelson, David; Ertel, Elizabeth  
**Subject:** FW: follow up: child exploitation on Internet

Kelli Andrews  
 Majority Counsel  
 Committee on Energy & Commerce  
 Oversight & Investigations  
 316 Ford House Office Building  
 Washington, DC 20515

202/226-2424 (phone)  
 202/226-2447 (fax)

-----Original Message-----

**From:** MacCarthy, Mark [mailto:MMacCar@visa.com]  
**Sent:** Tuesday, June 06, 2006 2:51 PM  
**To:** Andrews, Kelli  
**Subject:** RE: follow up: child exploitation on Internet

Kelli, here's some follow up information

1) The number of new CP sites being identified that say they accept Visa (actual or just displaying our marks) is decreasing.

2002 - 326  
 2003 - 517 (Number went up due to fine tuning of Internet search spider)  
 2004 - 175  
 2005 - 132  
 2006 - 68 so far

2) We retest the sites that we have identified as CP and that say they are accepting Visa. Some have managed to slip back in; some we have kept open at the request of law enforcement. But the percentage of these retested CP web sites that are no longer available or that do not accept Visa is increasing.

2002 - 70% of sites re-tested are no longer available or no longer accept Visa for payment.  
 2003 - 81%  
 2004 - 88%  
 2005 - 91%  
 2006 - 94%

Let me know if you have any further questions.

Mark MacCarthy  
 Senior Vice President, Public Policy  
 Visa U.S.A., Inc.  
 1300 Connecticut Avenue, NW  
 Suite 900  
 Washington, DC 20036  
 202 296-9230  
 mmaccar@visa.com

-----Original Message-----

**From:** Andrews, Kelli [mailto:Kelli.Andrews@mail.house.gov]  
**Sent:** Thursday, June 01, 2006 11:12 AM  
**To:** MacCarthy, Mark



Subject: RE: follow up: child exploitation on Internet

Mark:

I actually need the breakdown per each year in which you searched:

2002  
2003  
2004  
2005

And any information you have for 2006.

Please provide me with all of that information as soon as possible. It's probably best to do it via email.

Thanks-  
Kelli

Kelli Andrews  
Majority Counsel  
Committee on Energy & Commerce  
Oversight & Investigations  
316 Ford House Office Building  
Washington, DC 20515

202/226-2424 (phone)  
202/226-2447 (fax)

-----Original Message-----

From: MacCarthy, Mark [mailto:MMaccar@visa.com]  
Sent: Thursday, June 01, 2006 11:05 AM  
To: Andrews, Kelli  
Subject: RE: follow up: child exploitation on Internet

Kelli,

Here are some numbers for you. Our current search company is G2. They do the searches for us using criteria we define and then we bring the results in house to decide what to do. Call with questions.

\* Web pages searched per day 24X7 looking for the Visa brand and marks

in association with child abuse commerce - 11+Million

\* URLs of suspected child abuse sites and which appear to be accepting

Visa cards, provided to law enforcement in 2005 - 2200

\* Web sites meeting Visa definition of child abuse and which are accepting Visa for payment of child images abuse; in 2002 - 326, in 2005

-  
132

-----Original Message-----

From: Andrews, Kelli [mailto:Kelli.Andrews@mail.house.gov]  
Sent: Wed May 31 07:00:01 2006  
To: MacCarthy, Mark  
Subject: RE: follow up: child exploitation on Internet

I need to talk to you about the questions below. Please let me know when you have those exact figures (your message you left me said the #'s were going down)--I'd like more specifics as I mention below.  
There is no hearing involving the financial co's set yet.

Please let me know a time when you can discuss specific #'s to the questions below.

Thanks-

Kelli

Kelli Andrews  
Majority Counsel  
Committee on Energy & Commerce  
Oversight & Investigations  
316 Ford House Office Building  
Washington, DC 20515

202/226-2424 (phone)  
202/226-2447 (fax)

-----Original Message-----

From: MacCarthy, Mark [mailto:MMaccar@visa.com]  
Sent: Tuesday, May 30, 2006 4:24 PM  
To: Andrews, Kelli  
Subject: RE: follow up: child exploitation on Internet

Any further developments on this? Do you need more info from us? Is a hearing scheduled?

-----Original Message-----

From: Andrews, Kelli [mailto:Kelli.Andrews@mail.house.gov]  
Sent: Wed Apr 26 14:45:25 2006  
To: MacCarthy, Mark  
Subject: follow up: child exploitation on Internet

Mark:

I understand you are out of the office until Friday and I wanted to let you know the follow-up questions I had regarding the sexual exploitation of children over the Internet. I'd like to get a better understanding of why Visa pulled out of the Match system many years ago. It is my understanding that this is a massive database of terminated merchants that both m/c and amex are a part of and share information about. Can you also provide us some figures on the monthly/yearly hits that you get on suspected cp sites (I know you are simply looking initially at the IP issue) but we'd be interested in the break-down b/w how many IP hits you get and then from those, how many are suspect cp sites, and then from those, how many actually do seem to accept visa (with test transaction)?

Thanks so much-

Kelli

Kelli Andrews

Majority Counsel

Committee on Energy & Commerce


Oversight & Investigations

316 Ford House Office Building

Washington, DC 20515

202/226-2424 (phone)

202/226-2447 (fax)



## Membership 40 days for \$60

### Children's Dreams JOIN PAGE




## Registration Form

We are strongly recommending, do not to rush into E-gold purchase because it is very easy and conveniently to access almost all kind of e-gold payment system. First of all you stay absolutely anonymous. Second, it is a simple as ordinary credit card payment.

**E-gold is...**  
E-gold is an electronic currency, issued by e-gold Ltd., a Nevis corporation, 100% backed at all times by gold bullion in allocated storage.

Other e-metals are also issued: e-silver is 100% backed by silver, e-platinum is 100% backed by platinum, and e-palladium is 100% backed by palladium. However, the most popular e-metal (by an overwhelming margin) is e-gold.

e-gold is integrated into an account based payment system that empowers people to use gold as money. Specifically, the e-gold payment system enables people to Spend specified weights of gold to other e-gold accounts. Only the ownership changes - the gold in the treasury grade vault stays put.

**As simple as 1-2-3.**

**STEEP 1:**  
You should open E-gold account click here.  
(If you already have E-gold account, you can skip this chapter).

**STEEP 2:**  
Then you must add money to your Egold account.  
If you are new to egold please read information at <http://www.egoldeasy.com/> there you may easily create Egold account and add money to your Egold account from credit card and many other ways at <http://www.egoldeasy.com/>

**Remarks:** The first time you add money, you will have to be verified. They do this by calling you on either your home or mobile telephone. This is nothing to worry about!! Usually a man called Paul will call you from Australia. All he will ask you is your name. He won't be any problem!! After the call he will credit your account. After that, you can just add money whenever you like, without need for confirmation. **It's as easy as that!!**

**STEEP 3:**  
When you have money on your e-gold account simply complete payment. Fill form (right on page) and confirm payment. We will review the information and send you your login and password as

**You need to have E-Gold account to processing**

**Website:** **Children's Dreams (Members Area)**

**Amount:** **USD 69.00**

**You are purchasing a 40 days subscription.**

**Your Account Number:**

**Your Name:**

**Email:**

**Secure Purchase**

If you don't have an E-gold account, please click here

If you have any questions please contact our support team.

If you want to fund your E-Gold account follow this link.

**Here to stay**

E-gold is always as good as the gold it's backed with - this year, next year, a thousand years from now.

**Trustworthy**

Pursuant to the e-gold Account User Agreement, the physical bullion that comprises the value backing e-gold must be insulated from physical, legal and political risks. Title is held by The e-gold Bullion Reserve Special Purpose Trust that exists for the express purpose of holding bullion for the exclusive benefit of all e-gold account holders collectively. The bullion is held in the form of certified good delivery bars in allocated storage at repositories certified by the London Bullion Market Association (LBMA). Metal is held free of any lien or encumbrance whatsoever and explicitly may not be attached to any liabilities of e-gold Ltd. or any other entity. No metal may be removed from storage or any other disposition made without the signatures of both e-gold Ltd. and a third party Escrow Agent of good reputation.

soon as possible. Usually transaction time takes from 2 up to 12 hours. Please be patient.

**REMEMBER!**

Our preview pages can be deleted, moved, renamed. Process of funding your account can take 24-48 hours. We recommend remember or save anywhere our main e-mail address. If you'll have problems to access this payment page or if you have any questions please contact our support team.

Thank you

**No barriers to entry**

It costs nothing to open an e-gold account.

There is no credit check.

There is no minimum balance requirement.

There is no concept of a "merchant account" in that all e-gold accounts may Spend e-gold or receive e-gold payments.

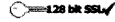
In short, you are minutes away from opening your first e-gold account at:

**Better money**

Free Web Hosting by 100FREE.COM. Visit Our User Forum. Visit Modelplace. Visit The Best Free Image Hosting.



Secure payment services provided by **e-gold®** on behalf of  
**STUDIO Dreams**



No e-gold account?  
**Sign up now!**

To pay directly from your e-gold® account, fill out this payment order form and press the **Preview** button.

<b>e-metal® payment order</b>	
Pay: <b>3236670 (STUDIO Dreams )</b>	
Amount: <b>69.00</b>	
USD ' worth of	<input type="text"/> Gold
Memo: <input type="text"/>	
_____ Authorize Payment	
From:	<input type="text"/> (Account Number)
Passphrase:	<input type="text"/>
Turing Number:	<input type="text"/> <b>88993/4</b>
Enter sequence of numbers displayed in grid directly above. <b>Audible Turing Number</b>	

After clicking Preview, you will be presented with a summary of the transaction you have entered.  
At that point you may choose to Confirm this e-metal spend.  
Once you confirm an e-metal spend, you can not reverse the transaction and take your e-gold back.  
(See [non-repudiation policy](#))

This **e-gold** payment order requires that cookies be enabled on your browser to function properly.  
Would you like to have an **e-gold** checkout button on your web site? [Visit the e-gold® programmer's page](#)

6/1/2006 6:31:32 PM GMT

© 2005 e-gold Ltd.



Land Rover LR3  
Click here to see how

LOCATE A RETAILER VISIT LANDRO

**BusinessWeek** online

TOP NEWS | GW MAGAZINE | INVESTING | ASIA | EUROPE | TECHNOLOGY | AUTOS | INNOVATION | SMALL BIZ | B-SCHOOL

JANUARY 9, 2006  
INVESTIGATIVE REPORT

**Get Four Free Issues**

Register  
Subscribe to BW  
Customer Service

Full Table of Contents  
Cover Story  
Up Front  
Readers Report  
Corrections & Clarifications  
Technology & You  
Voices of Innovation  
Media Center  
Business Outlook  
The Business Week  
Washington Outlook

## Gold Rush

Online payment systems like e-gold Ltd. are becoming the currency of choice for cybercrooks

Crime courses through the internet in ever-expanding variety. Hackers brazenly hawk stolen bank and credit-card information. Pornographers peddle pictures of little boys and girls. Money launderers make illicit cash disappear in a maze of online accounts. Diverse as they are, many of these cybercriminals have something important in common: e-gold Ltd.

**Get 4 FREE Issues!**

**STORY TOOLS**

- Printer-Friendly Version
- E-Mail This Story
- Reader Comments



**TC POP**

1. Sec
2. Sec
3. Sui
4. Mo
5. The

Get Free

**MARKET**

DJIA  
S&P 500  
Nasdaq

**RELATED ITEMS**

Graphic: E-Gold's Stash  
Graphic: Moving Money The E-Gold Way  
Graphic: Golden Touch  
Money Ain't What It Used To Be  
Graphic: Back To The Future?  
Online Extra: Dr. Jackson's Golden Vision  
Online Extra: WebMoney and Its Customers

**STOCK**

Stocks  
Korea I  
Create / Launch

\$9.95 RL EQ

Asian Business  
European Business  
Global Outlook  
News: Analysis & Commentary  
Special Report  
Working Life  
Legal Affairs  
People  
Science & Technology  
Investigative Report  
Finance  
The Corporation  
Personal Business  
Plus  
Inside Wall Street  
Figures of the Week  
Ideas -- Books  
Ideas -- Face Time With Maria Bartiromo  
Ideas -- Editorials

**INTERNATIONAL EDITIONS**

International -- Editor's Memo  
International -- Corrections & Clarifications  
International --

ADVERTISEMENT

Unavailable Video

SOUND

EXPERIENCE ALL NEW DRIVE IT G

JAGUAR

E-gold is a "digital currency." Opening an account at [www.e-gold.com](http://www.e-gold.com) takes only a few clicks of a mouse. Customers can use a false name if they like because no one checks. With a credit card or wire transfer, a user buys units of e-gold. Those units can then be transferred with a few more clicks to anyone else with an e-gold account. For the recipient, cashing out -- changing e-gold back to regular money -- is just as convenient and often just as anonymous.

E-gold appeals to "gold bugs": people who invest in the precious metal and believe money ought to be anchored to it. E-gold boasts that its digital currency is backed by a stash of gold bars stored in London and Dubai. But e-gold also appeals to

Developments to Watch  
International -- Global  
Figures of the Week

#### BUSINESS DIRECTORY

Stop searching,  
start finding!

Accounting  
Advertising &  
Marketing  
Air Charter  
Annuities  
Antivirus / Antispan  
Solutions  
Architects

POWERED BY  
DIRECTORY 311

#### PREMIUM CONTENT

MBA Insider

#### BW MAGAZINE

Get Four Free Issues  
Register  
Subscribe  
Customer Service

#### ONLINE FEATURES

Book Reviews  
BW Video  
Columnists  
Interactive Gallery  
Newsletters  
Past Covers  
Philanthropy  
Podcasts  
Special Reports

#### BLOGS

Auto Beat  
Blogspotting  
Brand New Day  
Byte of the Apple  
Deal Flow  
Economics Unbound  
Fine On Media  
Hot Property  
Investing Insights  
New Tech in Asia  
NussbaumOnDesign  
Tech Beat  
Working Parents

#### TECHNOLOGY

J.D. Power Ratings  
Product Reviews  
Tech Stats

savvy online crooks who want to move money quickly and without detection. American banks and conventional cash transmitters like Western Union are legally required to monitor customers and report suspicious transactions to the government. E-gold seems to go out of its way to avoid such obligations. Its operations are in Florida, but in 2000, its principals registered the company in the lightly regulated Caribbean haven of Nevis.

Law enforcement officials worry that the little-known digital currency industry is becoming the money laundering machine of choice for cybercriminals. On the evening of Dec. 19, agents with the Federal Bureau of Investigation and Secret Service raided the Melbourne (Fla.) office of e-gold's parent company, Gold & Silver Reserve Inc., and the nearby home of its founder, Douglas L. Jackson. Agents copied documents and computer files, but so far no charges have been brought. The Secret Service and the FBI declined to comment on the raid. Jackson has denied any wrongdoing, though the raid isn't the first indication that federal investigators view e-gold as a magnet for online misdeeds. The FBI separately is pursuing about a dozen probes in which e-gold appears as a "common denominator," a senior agent says.

The potential danger goes beyond e-gold. Investigators say other digital currencies are similarly used for corrupt purposes. All told, there are at least a dozen such services worldwide, based in places like Russia and Panama. Eight of them, including e-gold, claim to be backed by actual bullion. As a group, these firms do billions of dollars a year in transactions, according to Jim Davidson, a spokesman for the Global Digital Currency Assn. in New York. E-gold and its rivals make money by charging small percentage fees on those transactions.

Most of the law enforcement interest in e-gold involves alleged fraud and money laundering by its users. A tour of some outlaw corners of the Internet illustrates why. One Web site called CC-cards -- where cyberthieves sell pilfered bank account and credit-card information -- often asks for payment via e-gold. Some sites pushing child pornography have dropped Visa and MasterCard recently in favor of e-gold, according to the National Center for Missing & Exploited Children, which tracks underage porn.

But U.S. officials have another concern: that e-gold and rival digital currencies could be used to finance terrorism. It's a notion the companies all reject.

#### SUBPOENA CENTRAL

The man behind e-gold, Doug Jackson, is a tall, powerfully built former oncologist. A fan of the gold standard, Jackson, 49, became a pioneer in digital currency when he set out a decade ago to create what he describes as a private gold-based monetary system. He envisioned e-gold as a currency that would be accepted at Wal-Mart (WMT) while also permitting peasants from China to Peru to offer products at stable prices. "I thought there would be this flock of e-gold users, and I would be their messiah," he says. "It just didn't happen."

What did happen, according to law enforcement officials, was that a pack of felons flocked to Jackson's brainchild. Sitting in an undecorated conference room in the Melbourne office three months before the federal raid, he acknowledged that he had a "six-inch pile" of subpoenas from such agencies as the FBI, the Securities & Exchange Commission, and the U.S. Postal Inspection Service -- all seeking information about some of his more suspect customers. Investigators say Jackson may have begun his quirky business with innocent intentions. But in recent years he has turned a blind eye, the officials say, to mounting evidence that e-gold has attracted a seamy clientele. The federal raid suggests that agents are intensifying their focus on e-gold and its potential criminal liability.

Jackson didn't respond to messages after the raid. But earlier, he denied

Wildstrom: Tech Maven
<b>AUTOS</b>
Home Page
Auto Reviews
Classic Cars
Car Care & Safety
Hybrids
<b>INNOVATION &amp; DESIGN</b>
Home Page
Architecture
Brand Equity
Auto Design
Game Room
<b>SMALLBIZ</b>
Smart Answers
Success Stories
Today's Tip
<b>INVESTING</b>
Investing: Europe
Annual Reports
BW 50
S&P Picks & Pans
Stock Screeners
Free S&P Stock Report
<b>SCOREBOARDS</b>
Hot Growth 100
Mutual Funds
Info Tech 100
S&P 500
<b>B-SCHOOLS</b>
Undergrad Programs
MBA Blogs
MBA Profiles
MBA Rankings
Who's Hiring Grads
<b>BW EXTRAS</b>
BW Digital
BW Mobile
BW Online Alerts
Dashboard Widgets
Podcasts <b>RSS 2.0</b>
RSS Feeds <b>RSS 2.0</b>
Reprints/ Permissions
Conferences
Investor Workshops
Research Services

vehemently that he has looked away from crime. He said he responds as quickly as possible to official inquiries. He acknowledged, though, that his staff of 15 includes only one in-house investigator who struggles to keep up with all those subpoenas. E-gold has about 1.2 million funded accounts through which transactions worth \$1.5 billion were conducted in 2005, he says. As for the idea that he should systematically monitor customer identities and money flows, he argues that's not his job: "We don't validate because we're unlike any other system."

Federal officials reluctantly confirm this loophole: E-gold and other digital currencies don't neatly fit the definition of financial institutions covered by existing self-monitoring rules established under the Bank Secrecy Act and USA Patriot Act. "It's not like it's regulated by someone else; it's not regulated," says Mark Rasch, senior vice-president of the Internet security firm Solutionary Inc. and former head of the Justice Dept.'s computer crime unit. The Treasury Dept.'s Financial Crimes Enforcement Network (FinCEN) is studying ways to close the regulatory gap. Meanwhile, U.S. officials say e-gold and similar companies should voluntarily do more to deter crime.

Started in 1996, e-gold was part of an early wave of Internet payment systems that converted conventional money into a Web currency. Most of those pioneers soon flopped, because consumers resisted paying fees to get Web cash. Others, such as PayPal, now a unit of online auction giant eBay Inc. (**EBAY**), evolved into credit-card processing services.

E-gold and a handful of rivals, including one called GoldMoney, were different. Their founders believed that tying monetary exchange to a strict gold standard would achieve greater economic stability. The Internet provided a ready venue for gold bugs the same way that it offered a soapbox to adherents of every other strain of thought. Jackson, an Army veteran and a graduate of Pennsylvania State University's medical school, was practicing oncology in Melbourne in the mid-1990s when he began reading about libertarianism and monetary theory. The married father of two adopted boys began to change his thinking. He scoured the works of libertarian novelist and philosopher Ayn Rand and was impressed by economist Friedrich A. Hayek's *The Road to Serfdom*, an influential 1944 condemnation of government control of the economy. "It looked like a lot of the suffering of recent centuries -- some of the scale of wars, some of the economic dislocations -- could be traced back to credit cycles. And credit cycles could be traced back to monetary manipulation" by governments, Jackson says. "I was very moved by it."

#### INTELLECTUAL CONVERSION

Gold, he concluded, was the cure. The U.S. stopped tying the dollar to a fixed amount of gold in 1971. But Jackson and a friend, attorney Barry K. Downey, decided to start what amounted to their own gold-backed currency. Jackson liquidated retirement accounts and sold his medical practice to help raise an initial \$900,000. A former colleague noticed him working on computer code around the clock at his stand-up doctor's desk. He often forgot to eat and lost weight. Along the way, he stopped attending church. Jackson confirms all this but stresses that he continued to provide excellent care for his patients until he bowed out of medicine completely in 1998.

In a series of interviews with Jackson, his statements about e-gold swing from grandiose to resigned. "We want e-gold to be recognized as a privately issued currency and to be treated as a foreign currency" by the U.S. and other governments, he says at one point. But e-gold's offices don't conjure up images of a grand central bank. Jackson, who during one interview wore neatly pressed slacks and a yellow-striped shirt, runs his currency from a Spartan suite on the



third floor of a Bank of America (BAC) building.

Online currencies are patronized by software companies and other small businesses. Jackson says that the fees he charges customers -- for converting real money to e-gold, administering accounts, and doing transfers -- generated about \$2 million in revenue in 2005 for e-gold's parent company, Gold & Silver Reserve, which he also controls. The operation turns a profit, he adds, but he won't say how much.

Mark Jeftovic considers himself a big fan of digital currencies -- but one now skeptical about e-gold. The founder of easyDNS Technologies Inc., an Internet domain name registrar in Toronto, he started accepting e-gold as payment in 2003. Jeftovic believes that digital currencies will minimize the harm of government-induced inflation. But in early 2005, investigators from the Royal Canadian Mounted Police visited easyDNS seeking information about cybercriminals allegedly using the registrar's services. It turned out that some of the suspects had paid Jeftovic's company via e-gold, he says. Angered by the police scrutiny, Jeftovic now plans to offer rival digital currency GoldMoney in addition to e-gold. "I like the digital currency and e-gold economy, and I want to support it," he says. "But you have to run a cleaner shop than this."

The RCMP didn't respond to requests for comment. Jackson says he wasn't aware of Jeftovic's concerns or the RCMP investigation. He says that e-gold responds as quickly as possible to inquiries from law enforcement agencies and readily provides them with user names, account numbers, and transaction histories.

A number of gold buffs and some law enforcement officials see GoldMoney as a reputable alternative in the digital currency field. Based in the British Channel island of Jersey, GoldMoney is run by James Turk, a precious metals trader and former Chase Manhattan banker. He says that his company requires new customers to mail in copies of identity documents and then checks the data against lists of suspected terrorists and money launderers. The accounting giant Deloitte & Touche annually audits its gold holdings and security measures.

E-gold's Jackson says those steps are expensive and unnecessary. OmniPay, an affiliate of e-gold, is one of more than a dozen "digital currency exchange agents" that handle the conversion of conventional currency into e-gold. Jackson says that to authenticate users' identities, OmniPay sends them a special code via e-mail and conventional mail. But users aren't required to prove their identity, so it isn't clear what this accomplishes. Jackson says that his lone in-house investigator looks for obvious fraud, such as a customer using "China" as his only address.

Some of e-gold's customers have been unsavory. Omar Dhanani used e-gold to launder money for the ShadowCrew, a cybercrime gang with 4,000 members worldwide, according to an October, 2004, affidavit by a Secret Service agent. Based in a stucco house in Fountain Valley, Calif., Dhanani used his PC to hide the money trail from the sale of thousands of stolen identities, bank accounts, and credit-card numbers, the government said. Accomplices sent him Western Union (FDC) money orders, which, for a fee, he filtered through e-gold accounts. On Oct. 4, 2004, Dhanani, 22, who used the nickname Voleur -- French for thief -- boasted in a chat room that he moved between \$40,000 and \$100,000 a week. He pled guilty in November to conspiracy to commit fraud and faces up to five years in prison.

#### "GOOD FENCES"

E-gold's Jackson says the company was never contacted by the Secret Service regarding Dhanani and had no duty to sniff him out. E-gold's outside attorney, Mitchell S. Fuerst, calls statements in the Secret Service affidavit alleging that e-gold was used to facilitate illegal activity "nonsense." Fuerst argues that the

responsibility for policing the identity and activities of e-gold account holders lies with the banks and other regulated institutions from which money is transferred into e-gold's system. Jackson goes further, insisting it's impossible to launder money through e-gold -- a contention that law enforcers say is contradicted by the Dhanani case and others.

Jackson has made no secret of his desire to avoid U.S. government scrutiny. In 2000, he and his partner Downey registered e-gold Ltd. in Nevis, hoping the maneuver would add another layer of insulation from U.S. regulation. Jackson concedes that e-gold has existed in Nevis only as "a piece of paper." Its parent administers e-gold services from the Melbourne office; the operation's computer servers are in Orlando. Jackson says he chose the tiny island because registration there is inexpensive, and the government follows well-established British commercial law. Nevis is also known for lax financial regulation. Referring to his desire to create legal distance from U.S. officials, Jackson says: "There's an element of good fences make good neighbors."

On Dec. 5, two weeks before the federal raid in Melbourne, the Nevis Financial Services Regulation & Supervision Dept. posted a notice on its Web site that e-gold had disseminated "misleading information" about its legal status. Nevis officials say that the company was removed from the island's corporate registry in July, 2003, for failure to pay the annual registration fee of \$220. Jackson didn't respond to questions about this.

Back in the U.S., e-gold has tried to shield itself semantically, avoiding basic banking terms such as "deposit" and "withdrawal" that could increase its risk of being categorized as a regulated financial institution. E-gold calls such transactions "in-exchange" and "out-exchange." Jackson says: "It's not a desire to be tricky. It's a desire to be accurate. It's important not to be misconstrued as a bank."

Whatever its legal status, e-gold's usefulness to scam artists was colorfully illustrated by E-Biz Ventures, which allegedly portrayed itself as a Christian-influenced organization that offered investors returns as high as 100%. E-Biz' proprietor, Donald A. English of Midwest City, Okla., allegedly highlighted his reliance on e-gold to appeal to victims' fear of the federal government and their desire for anonymity. E-Biz investors opened e-gold accounts and transferred funds to accounts controlled by English. He shifted e-gold among more than 25,000 accounts, using new investors' money to pay off some older ones. The scam took in \$50 million before the SEC shut it down in 2001. Investors lost \$8.8 million. Later prosecuted in federal court in Oklahoma City, English pled guilty to wire fraud and last May was sentenced to five years in prison.

Jackson says that when subpoenaed by the SEC in the civil part of the E-Biz case, e-gold supplied transaction data. A Jackson aide worked closely with investigators in the civil case. "They responded timely to every request for assistance," says Chris Condren, E-Biz' court-appointed receiver.

Evidence of e-gold's suspect following is found on numerous Web sites. A contributor to Cannabis Edge, a site for marijuana growers, has provided advice on how to employ e-gold and two other digital currencies -- WebMoney and NetPay -- to hide illicit proceeds "beyond the reach of U.S. pigs." E-gold in particular "has strong security," is "easy to use, and is anonymous," said the writer, who used the name Bill Shakespeare. (Moscow-based WebMoney and NetPay, which is based in Panama City, Panama, both deny any wrongdoing.)

In addition to its abundant offerings of stolen financial data -- with payment frequently sought via e-gold -- the site CC-cards carried a message in November from a hacker using the name HellStorm. He advertised that for a 5% fee, he would set up and fund e-gold accounts for those who are in a hurry to do business

and want to shield their identity. Users of CC-cards can make donations for the upkeep of the site by clicking on a link that connects to an e-gold account. (E-mails seeking comment from CC-cards and Cannabis Edge weren't answered.)

Jackson says that he wasn't aware that e-gold was being recommended or used on outlaw Web sites until he was so informed by *BusinessWeek*. The company has since blocked the CC-cards donation account, he says. There is little the company can do about such situations, Jackson contends, unless law enforcement brings them to e-gold's attention. Once informed, "we can set a value limit to prevent an account from receiving further payments," he says. "We can identify if there is a constellation of accounts controlled by the same miscreant." Jackson adds: "If we get an appropriate court order, we can monitor and assist in a sting that freezes value."

The danger of Web sites like CC-cards that are fueled in part by e-gold became very apparent to Kimberly S. Troyer. Her identity went up for sale there last September. Among the 22 items CC-cards put on the block: her checking account number at Bank One (JPM ), driver's license number, Social Security number, birth date, and mother's maiden name. The price for all that: \$30 of e-gold. Informed of the offer by *BusinessWeek* in December, Troyer, a 33-year-old accounting student at Davenport College in South Bend, Ind., is changing all of her identity documents. She believes she escaped without losing any money. But someone hijacked her e-Bay account and changed the address to one in China so that it could receive payments from the sale of iPods Troyer didn't own. "It makes me sick to my stomach," she says. Jackson says e-gold can't do much about such cases until he's formally alerted by the government.

There is one crime, however, to which Jackson has reacted more aggressively: child pornography. In August, he attended a conference in Alexandria, Va., organized by the National Center for Missing & Exploited Children. The center is trying to enlist banks and credit-card companies in a crackdown on payment schemes used by child porn Web sites. "There are fewer and fewer sites with Visa -- and more and more with e-gold," says the center's chief executive, Ernest E. Allen. The center has a policy of not publicly identifying child porn sites it tracks. Jackson says he was appalled to find e-gold on the list of institutions used by the porn sites. He provided the center with instructions on how to seek e-gold records, and the group says it is pleased with e-gold's cooperation.

Daniel J. Larkin, head of the FBI's Internet Crime Complaint Center, says that in recent years, e-gold has hidden behind "a plausible-deniability fog." Now the fog may be lifting as the subpoenas pile up and federal agents begin to examine what they confiscated in their Dec. 19 raid. The Internal Revenue Service is separately auditing e-gold's parent, and Jackson says e-gold has voluntarily agreed to cooperate with an IRS review of its procedures for preventing money laundering. The IRS declined to comment.

#### **TERROR TOOL?**

Before the recent raid, Jackson said that responding to subpoenas and other government inquiries has been distracting and expensive. Although he emphasized that e-gold isn't obliged to monitor its clientele, he said that he could have paid more attention to vetting account holders were it not for the outside interruptions. He added that he plans to switch from an account-based log-in system to a user-based one to monitor customers more closely.

The worst-case scenario, so far undetected by officials, would be the use of e-gold by financiers of terrorism. Experts on terrorism funding note that digital currencies resemble the money-changing system known as hawala, which Middle Eastern terrorists have used. A customer gives money to a hawala service, which then

telephones a similar service in another city or country that doles out money to a designated recipient. Many hawala outfits have been shut down since September 11, making digital currencies a logical next step, says Phil Williams, a professor of international affairs at the University of Pittsburgh and consultant to the United Nations on terrorism financing. "At some point, this is going to be used" by terrorists, Williams says.

Jackson scoffs at this notion. "We are not bad guys, and the e-gold system simply does not pose an undue risk for usage for terrorist purposes," he wrote in an e-mail on Jan. 20, 2005, to AUSTRAC, Australia's anti-money-laundering regulator, which was looking generally into potential terrorist use of digital currency.

But e-gold attorney Fuerst said in early December that the company quickly complied with requests in 2005 from Russian law enforcement and the FBI for records connected to a would-be terrorist in Russia. This person allegedly threatened to "blow something up," Fuerst said, unless a ransom was paid into his e-gold account. The FBI and the Russian Interior Ministry declined to comment.

This month's raid could signal serious trouble for e-gold. But cybercrime experts predict that if the company falters, nefarious business will simply transfer to other digital currencies, especially ones based in countries that have lax law enforcement. Amir Orad, executive vice-president of cybersecurity firm Cyota, says that putting e-gold out of business "would not stop anything."

#### READER COMMENTS

#### Most recent comments

See all comments

Leave your own comments

**Nickname:** steve

**Review:** E-gold is a blessing for those who stay in countries that are not accepted by PayPal. PayPal is trying to monopolize the e-commerce business via Ebay. And Ebay does not even allow E-gold to be used in their transactions. Is that fair of Ebay? Isn't it biased to push PayPal when there are other payment types out there like moneybookers, alertpay, goldmoney, pecunix...and so on. Nobody can control the internet and that is the beauty of cyberspace...

**Date reviewed:** Jun 4, 2006 7:43 AM

**Nickname:** Jim

**Review:** Two words: Hegelian Dialectic. Whats the real motive for all these investigations? Internet taxation/regulation under the guise of protecting consumers.

**Date reviewed:** May 30, 2006 1:00 PM

**Nickname:** american little person

**Review:** What happened to payko, bidpay.com, pppay.com? Why can't foreign buyers pay in U.S. dollars? My poor mom helping individuals build a hospital in India can't even get U.S. dollars for the money she's loaned. No American Express travelers checks, no money gram, no Western Union, even bank transfers don't work. It's been three months waiting for a bank transfer to arrive from India but you can send them money in less than 3 days! Why can't an Indian send her a money order?

**Date reviewed:** Apr 1, 2006 10:17 AM

**Nickname:** american little person

**Review:** I'm sick of paypal. It's gotten more and more difficult to use and there are too many fees. If you don't accept their fees you are very limited in auction sales.

By Brian Grow, with John Cady, Susann Rutledge, and David Polek in New York



Copyright 2006 The McGraw-Hill Companies, Inc. All Rights Reserved

**BusinessWeek** online

Business Week Online

January 3, 2006 Tuesday

**SECTION: BUSINESSWEEK MAGAZINE****LENGTH:** 1473 words

**HEADLINE:** Online Extra: Dr. Jackson's Golden Vision;  
The founder of e-gold discusses identity theft, regulatory compliance, and his libertarian epiphany

**BODY:**

When he founded e-gold in 1996, Dr. Douglas Jackson, a former oncologist, had a grand vision. He believed his digital currency -- housed on the Internet, backed by gold bullion, immune to inflation and currency fluctuations -- would "improve the material welfare of mankind." Users could convert national currencies into e-gold, then buy and sell goods with any other e-gold account holder worldwide over the Web.

Since then, that noble endeavor to create a new kind of money has gone seriously awry, according to U.S. law-enforcement officials. While a smattering of small businesses in the U.S. and overseas have adopted e-gold as a payment vehicle, U.S. investigators say many of its other customers have instead come from the dark side of the Internet.

Despite evidence that e-gold is now a favored currency among such nefarious characters as identity thieves and financial fraudsters, Jackson denies the claims and remains wed to the dream that e-gold will one day secure its place as currency for the Digital Age. In a series of interviews in person, by telephone, and via e-mail with BusinessWeek correspondent Brian Grow, Jackson offered his thoughts about the origin of e-gold, how it is regulated, and his effort to fend off critics.

Here are edited excerpts:

In 2000, e-gold Ltd. was registered as a company in Nevis, West Indies. Do you intend to bring it back to the U.S.?

I don't know. There's an element of "good fences make good neighbors." The cost of compliance can sometimes be very high in the U.S. The experience of PayPal is that they find themselves not dealing with one regulatory regime but with [multiple] regulatory regimes.

How does e-gold know who its customers are?

There are business reasons to know who a customer is, and then sometimes there are sort of nonsense reasons to know who a customer is. If you're trying to accept a money payment from somebody, you have to know who a customer is to accept a dollar payment from them. The nature of e-gold -- this is purposeful -- we want that finality of payment. As a result, there is nothing that the user can do that leaves e-gold on the hook.

Gold & Silver Reserve Inc., e-gold's parent company, also operates **OmniPay**, a digital currency-exchange agent that converts national currencies into e-gold. How does it authenticate the identity of its customers?

To do business with **OmniPay**, you have to establish a user profile. The [first step] is to make sure that someone controls the e-mail address that they're registering to the account. We send a secret to the e-mail address on file; they have to go back to the Web site and enter that secret.

Also, any e-gold account that they are going to use, they have to bind to that profile. They have to send a payment from that account to **OmniPay's** e-gold account. Another thing that's done is a postal validation. We mail out a secret to that postal address, [then] they have to log back into the Web site and enter that secret.

What's the philosophy behind e-gold?

My concern...was that historically it looked like a lot of the suffering of recent centuries -- some of the scale of wars, some of the economic dislocations -- could be traced back to credit cycles, and that credit cycles could be traced back to monetary manipulation. I wanted to try to create a system that was not subject to discretion, that was rules-based and predictable.

But how did you get to the point where you had researched suffering, traced it to credit cycles, and then decided to found e-gold?

There were a number of threads to it. At least one thread was just an interest in investing because, as a physician, I had some excess income, although I was a pretty lousy investor. Another strong theme of it -- and this is a little bit embarrassing -- was sort of a libertarian thing.

There was an article in Forbes in 1994, a sort of 50-year look back on Friedrich Hayek's book *The Road to Serfdom*. I had never read that book, [which condemns government meddling in the economy]. But [its] description was very compelling. [It] made reference to a bookshop in San Francisco called Laissez Faire Books. I got their catalog and started reading through the core works of the whole libertarian thing.

What it comes down to is the base money issuer [governments] -- that's the place where it is inappropriate to have a bank, in my opinion.

So, how does e-gold solve that problem?

By having a system like e-gold, what we were shooting for was to give the general public access to an efficient remote-payment mechanism without the need to go through an obligatory financial intermediary. That's fundamentally what it is all about.

What regulatory regime applies to e-gold? Are you a bank, a commodity, a financial instrument?

The simple answer is: We're nothing that's defined in legislation. Truth be known, we've looked very closely to see if we might be a money-service business, a money transmitter, because those have very distinct regulatory regimes, and also financial institutions and banks do. Clearly, we're none of those things. What we are trying to sort out right now is: Do we want to voluntarily emulate one of those things?

Is it an advantage not to be anything that's defined in legislation?

At the end of the day, we want e-gold to be recognized as a privately issued currency and treated like a foreign currency. Just as the U.S. doesn't presume to regulate the Reserve

Bank of India or Bank Negara Malaysia or the European Central Bank, we want e-gold to fall in exactly the same pigeonhole as a foreign central bank.

We want the regulatory focus to be on **OmniPay**, because **OmniPay** is where money or value -- as it's defined in regulation and legislation -- comes into play. We've been making the case that **OmniPay** is really not a money-service business either, but we are close enough to it that it makes sense for it to observe the spirit of the Bank Secrecy Act as it has been modified by the Patriot Act.

So **OmniPay** is not currently regulated as an exchange provider either?

Correct. The definition of an exchange involves money on both sides. In every currency exchange, there are two payments -- this one goes in and that one comes out. **OmniPay** is specifically set up so that it never crosses from one national currency to another. There is always going to be e-gold on one side or the other.

E-gold doesn't fit the existing definition of money. In fact, there is not a definition of money; there is a definition of currency. E-gold doesn't fit the definition of currency. Currency is issued by a sovereign entity.

Cybercrime gangs like ShadowCrew are masters of using false identities. How can e-gold make sure that they're not using false identities?

E-gold essentially doesn't need to. **OmniPay** has to, because it handles money. But e-gold doesn't need to, because [a customer] can come in and be Mickey Mouse. But we have his time stamps, his IP numbers, and we also know all of the other accounts he does business with. If his value is still in the e-gold, we're just itching to get the order to freeze it.

Do you ever have suspicions of activity going on in e-gold accounts that may not be legal?

Early on, we had that luxury. Now, generally, we wait until somebody tells us about trouble.

Why doesn't e-gold police its network more vigorously, instead of relying on law enforcement to inform it of wrongdoing?

Our obligation is to honor what we have described in the [e-gold] account user agreement: to maintain a 100% reserve for e-gold; to operate a system of transfers that is irreversible; we will exercise a right of association, if there is due process, we can take further action such as freezing accounts.

Some of these things get into the area of legal opinion and regulatory questions, which I believe are a little bit complex. We have been in this process of dialogue and discussion with [regulators] as we try to assess what is the appropriate way to regulate e-gold vis-a-vis U.S. regulations.

The 2003 National Money Laundering Strategy from the U.S. Dept. of Treasury states that an e-gold account may be opened with only an e-mail address, and that personal information does not appear to be verified. Is this accurate?

Correct. As noted by the World Bank, excess zeal in [know-your-customer rules] excludes many of the world's poor from the benefits of things like international remittances. We enable the guy living in the shantytown surrounding Mexico City to bootstrap himself, yet without occasioning a risk of someone getting away with truly anonymous abuses.

Is e-gold aware that cybercriminals are offering "funding" services to help others obtain e-

Browse Display

Page 4 of 4

gold?

No, but when made aware, we can aid in bringing hellfire down on their heads.

**LOAD-DATE:** January 3, 2006[◀ prev](#) Document 26 of 35 [next ▶](#)

---

[About LexisNexis™](#) | [Terms and Conditions](#) | [Privacy Policy](#) | [Support Identifier](#)  
Copyright © 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.



UNITED STATES OF AMERICA, :  
c/o United States Attorney's :  
Office :  
Judiciary Center Building :  
555 4th Street, N.W. :  
Washington, D.C. 20530, :  
:  
Plaintiff, :  
:  
v. :  
:  
ALL FUNDS SEIZED FROM OR :  
ON DEPOSIT IN SUNTRUST :  
ACCOUNT NUMBER xxxxxxxx8359, :  
IN THE NAME OF GOLD AND :  
SILVER RESERVE, INC. AND ALL :  
FUNDS ON DEPOSIT IN REGIONS :  
BANK ACCOUNT NUMBER :  
xxxxxx4851, IN THE NAME OF :  
GOLD AND SILVER RESERVE, INC. :  
:  
Defendant. :  
:  
:

Civil Action No.

2. This Court has jurisdiction over this matter by virtue of 28 U.S.C. §§ 1345 and 1355(a). Venue is established by virtue of 28 U.S.C. §§ 1355(b)(1) and 1391(b).

3. The defendant funds are:

- a. All funds seized from or on deposit in SunTrust Bank account number xxxxxxxx8359, in the name of Gold and Silver Reserve, Inc. ("SunTrust account"); and
- b. All funds seized from or on deposit in Regions Bank account number xxxxxx4851, in the name of Gold and Silver Reserve, Inc. ("Regions account").

4. On December 15, 2005, a seizure warrant was issued by this Court (J. Facciola), authorizing seizure by the United States Secret Service of all funds contained in these two accounts. The amount seized pursuant to the warrant from the SunTrust account was \$135,912.32 and the amount seized from the Regions account was \$590,306.59. The seized funds are currently in the custody of the United States Secret Service. An additional \$89,405.55 has since been deposited into the Regions account, and both accounts are still able to receive deposits.

5. The two bank accounts listed above are owned and operated by Gold & Silver Reserve, Inc. doing business as OmniPay ("OmniPay"), which is a company that offers to exchange United States (and several other countries') currency into E-Gold, a private "digital" or "electronic" currency offered through the internet ([www.e-gold.com](http://www.e-gold.com)) and purportedly backed by gold bullion. OmniPay provides three currency exchange services: (1) receiving national currency by wire for conversion into E-Gold; (2) converting E-Gold back into national currency (which may then be sent to the customer by wire transfer, check, or a bill paid to a third party on their behalf); and (3) conversion of E-Gold into another e-metal currency.

6. The term "electronic currency" has been adopted by Internet-based "sellers" of gold, silver, platinum, palladium, and other metals to describe the use of precious metals as a private currency for online payments. Issuers of electronic currencies promote the global acceptance of precious metals, observing that a buyer paying with gold does not have to worry about access to, or

acceptance of, underlying currencies. Merchants, online service providers, and individuals who are willing to receive payment in precious metals are allocated a quantity based on the day's market price. While taking delivery of the actual metal appears, technically, to be an option, recipients typically "sell" the metal through a digital currency exchanger and receive payment in a more conventional form by "cashing" out some portion of their digital currency accounts. Recipients can also transfer ownership of some or all of their precious metal holdings to someone else. This transfer of ownership of the underlying metal through the crediting and debiting of internet-based accounts is how online precious metal issuers facilitate payments on behalf of customers.

7. There are four primary steps involved in a financial transaction using a digital currency process (from the customer's perspective): (i) opening a digital currency account; (ii) converting national currency into a digital currency through an exchanger to fund the digital currency account; (iii) using value in the account to buy or sell a good or service; and (iv) exchanging value in the account back into national currency. Accordingly, digital currency issuers need two additional parties to complete these steps: (i) digital currency exchangers; and (ii) merchants that accept digital currencies for the payment of goods and services.

8. A person wishing to use a digital currency to purchase a good or service must first open an account with a digital currency issuer, which typically can be done online by providing only a valid email address. In order to fund a digital currency account, issuers typically require a customer to use the services of a third party digital currency exchanger. The exchangers generally operate independently from digital currency issuers. Exchangers provide services for customers wishing to engage in the buying, transferring, and selling of online precious metals. In particular, exchangers take national currency from customers and exchange it into a digital currency for purposes of funding, or increasing the value of, an existing digital currency account. By the same

token, exchangers also exchange the value in an account into national currency. Exchangers are typically the only method by which customers can obtain the value out of an account, short of taking possession of the precious metal itself. Each exchanger sets its own terms and conditions on the types and amounts of national currencies that will be accepted for exchange. Some only accept transfers from bank or credit card accounts. Others accept cash and money orders. Similarly, each exchange service offers different options for receiving funds. Some exchangers have physical locations, whereas others exist only virtually. There are many digital currency exchangers, including, OmniPay.

9. Gold & Silver Reserve, Inc. ("G&SR") d/b/a Omnipay, a Delaware Corporation incorporated on January 24, 1996 as an E-Gold transnational monetary payment system, is a digital currency exchanger that offers currency exchange services for individuals wishing to purchase, transfer, and/or sell E-Gold. The principle officers are Douglas Jackson, President, Reid Jackson, Director, and Barry Downey, Secretary. The business address of OmniPay is 175 E. Nasa Blvd., Suite 300, Melbourne, Florida. OmniPay operates via the Internet using the domain name [www.omnipay.com](http://www.omnipay.com).

10. According to the OmniPay and E-Gold websites, "Gold & Silver Reserve, Inc. (G&SR), a Delaware Corporation, developed and deployed the e-gold payment system in 1996, and through 1999 administered both payment settlement and currency exchange. In January 2000, the core e-gold roles of Issuance and Settlement were devolved to e-gold Ltd., a Nevis W.I. company created specifically to serve as the General Contractor responsible for performance of the e-gold Account User Agreement . . . This separation of roles was designed to further assure e-gold's freedom from default risk and finality of settlement by dissociating the e-gold Issuer from business risks relating to exchange. G&SR, Inc. continues to serve as Operator of the e-gold payment system,

as well as offering its own innovative set of hybrid currency exchange services, known as OmniPay.” E-gold, Ltd. is also operated by Douglas Jackson, Barry Downey, and Reid Jackson.

11. OmniPay provides customers with a mechanism to convert national currency into E-Gold, and E-Gold into national currency. OmniPay also offers a bill payment service for E-Gold customers. The home page of the OmniPay website describes OmniPay’s three primary services:

1. InExchange Service. The InExchange service changes national currency into a value associated with a particular e-metal.
2. M2M Service. The M2M service transfers value from one e-metal account to another e-metal account.
3. OutExchange Service. The OutExchange service changes the value in an e-metal account to national currency.

12. The terms “InExchange” and “OutExchange” are vernaculars for the traditional banking terms “deposit” and “withdrawal,” respectively. E-Gold account holders deposit funds into their E-gold account via OmniPay’s “InExchange” service, which permits a user to convert a national currency into an e-metal. Currently, OmniPay accepts national currencies from Canada, France, Germany, Japan, Switzerland, the United Kingdom and the United States for exchange. To fund an E-Gold account via OmniPay’s “InExchange” service, an individual opens an account with OmniPay by providing a valid email address (which is validated by OmniPay) a postal address, and a valid E-Gold account. OmniPay only accepts bank wires from account holders in the amount of \$1,000 or more to fund an E-Gold account. Once the wire is received by OmniPay, the customer’s E-Gold account is credited for that amount of gold. The E-Gold account will show the number of ounces available, not the dollar amount. The OmniPay website states that OmniPay accepts remittances through Federal Reserve Financial Services (*e.g.*, FedWire), Swift, and E-Gold. By accepting remittances only through bank wires (FedWire and Swift), OmniPay guarantees its receipt of funds from its customers and eliminates risks associated with other payment instruments, such as bounced

checks or counterfeit traveler's checks.

13. OmniPay's OutExchange service allows E-Gold account holders to withdraw value from their e-metal account into a national currency via bank wire or check. The following are the fees associated with the OutExchange Service:

<u>Type</u>	<u>Fee</u>
Check -- postal mail	\$1
Check -- courier	\$20
Bank Wire -- within US	\$20
Bank Wire -- outside US	\$40

E-Gold account holders can also exchange their E-metal for other E-metals using Omnipay's "M2M" service.

14. OmniPay also offers other services, including a bill payment service. An advertisement on the OmniPay website states: "Pay your bills with e-gold; Pay your mortgage, utilities, credit card, butcher, baker, candlestick maker - in short - all your bills with e-gold." When a customer wants to use the bill pay service, the customer accesses the OutExchange service and requests payment of a certain bill. OmniPay then debits the customer's E-Gold account and "converts" the corresponding value into currency. OmniPay will write a check to the creditor for a \$1 fee or send a domestic wire for \$20 (the fee for an international wire is \$40). OmniPay also receives a fee of 1% or 50 cents from the recipient of the payment.

15. G&SR receives 40% of all fee revenue generated by E-Gold where OmniPay acts as the exchanger. G&SR makes a market in the metals utilizing the bid/ask spread: that is, there is a 4% difference in the "In-Exchange" versus "Out-Exchange" rates. The OmniPay website at <http://www.omnipay.com/currentexchange.asp> provides a chart with Current OmniPay Exchange Rates and Fees for InExchange payments (i.e., deposits), OutExchange remittances (i.e.,

withdrawals), and metal to metal remittances (i.e., transfers).

16. Title 18, United States Code, Section 1960 provides that:

(a) Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

(b) As used in this section

(1) the term "unlicensed money transmitting business" means a money transmitting business which affects interstate or foreign commerce in any manner or degree and

(A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;

(c) the term "money transmitting" includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.

17. With regard to the registration requirements established in Section 1960(b)(1)(B), a money transmitting business is required to register by filing the appropriate information with the Financial Crimes Enforcement Network ("FinCEN"), an agency within the Department of Treasury.  
31 U.S.C. § 5330(a); 31 C.F.R. § 103.41(a)(1) and (b).

18. The District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., prohibits a person from engaging in the business of money transmission without obtaining a license

from the Superintendent. D.C. Stat. § 26-1002. Violation of the money transmitter statute is a felony with penalties of up to a \$25,000 fine and five years imprisonment. D.C. Stat. § 26-1023.

19. Under the D.C. Money Transmitters Act, the term “money transmission” is defined as “the sale or issuance of payment instruments or engaging in the business of receiving money for transmission or transmitting money within the United States, or to locations abroad, by any and all means, including but not limited to payment instrument, wire, facsimile, or electronic transfer.” D.C. Stat. § 26-1001(10).

20. The Florida Money Transmitter’s Code, Fla. Stat. §§ 560.101-560.408, prohibits a person from engaging in the business of a money transmitter without registering with the Office of Financial Regulation. Fla. Stat. § 560.125(1). Violation of the money transmitter statute is a felony. Specifically, the penalties for violating this statute are as follows: (1) if currency or payment instruments exceed \$300 but are less than \$20,000 in any 12-month period, the person has committed a third degree felony; (2) if currency or payment instruments total or exceed \$20,000 but are less than \$100,000 in any 12-month period, the person has committed a second degree felony; and (3) if currency or payment instruments total or exceed \$100,000, the person has committed a first degree felony. Fla. Stat. § 560.125(5)(a)-(c).

21. Under Florida Money Transmitters’ Code, the term “money transmitter” includes any person located in or doing business in Florida who acts as a payment instrument seller, foreign currency exchanger, check casher, funds transmitter, or deferred presentment provider.” Fla. Stat. § 560.103(11). The term “funds transmitter” includes “any person who engages in the receipt of currency or payment instruments for the purpose of transmission by any means, including transmissions within this country or to or from locations outside this country, by wire, facsimile, electronic transfer, courier, or otherwise.” Fla. Stat. § 560.103(10).



22. According to FinCEN records, no registration by Gold & Silver Reserve, Inc. d/b/a Omni Pay, EIN 58-2220023, had been filed for the period of December 31, 2001 through June 22, 2005. As of December 13, 2005, according to the FinCEN website at <http://www.msb.gov/guidance/msbstateselector.php>, which contains lists of businesses licensed as money transmitters with FinCEN in Florida and the District of Columbia (updated as of October 1, 2005), neither G&SR, OmniPay, nor E-Gold were registered as money transmitting businesses with FinCEN.

23. According to a Certificate of Record issued by the State of Florida, Office of Financial Regulation in July, 2005, there is no record of licensure or application for licensure on file by G&SR or OmniPay. As of December 13, 2005, according to the Florida Office of Financial Regulation website at <http://www.flofr.com/licensing/download.htm> (updated as of December 5, 2005), neither G&SR nor OmniPay were registered as money transmitting business within the State of Florida.

24. As of December 7, 2005, information from a Financial Institutions Examinations Officer at the Department of Insurance, Securities, and Banking in the District of Columbia indicated that a search of their databases had been conducted and that no record of license or registration as a money transmitting business had been found for G&SR and/or OmniPay in the District of Columbia.

25. Prior to February, 2005, G&SR d/b/a OmniPay held its operating accounts at Wachovia bank. On or about February, 2005, OmniPay closed its Wachovia accounts and opened Regions Bank account number xxxxxx4851, which became its main operating account for wire transfers. This is the account into which OmniPay customers are directed to send funds (by wire transfer over \$1,000) for exchange into E-Gold. Additionally, G&SR d/b/a OmniPay opened a

SunTrust account on December 7, 2004, which it uses to provide its exchange service for bill payment orders.

26. With respect to the primary wire account used by OmniPay at Wachovia Bank, from June 1, 2004 through February 8, 2005, over \$8.5 million was received in 430 incoming wire transfers and over \$8.7 million was sent in 238 outgoing wire transfers. These transactions involved incoming and outgoing wire transfers from and to other digital currency exchangers as well as individual customers.

27. With respect to Regions Bank account number xxxxxx4851 in the name of G&SR – Op. Wires, from February 4, 2005 through September 30, 2005, \$17,940,371.83 million was received in 839 incoming wire transfers and over \$17,519,899.42 million was sent in 460 outgoing wire transfers from and to other digital currency exchangers as well as individual customers. This activity, as well as the instructions posted on OmniPay's website, indicate that this account is being used as OmniPay's primary account for incoming and outgoing wires of currency.

28. With respect to SunTrust Bank account xxxxxxxx8359 in the name of G&SR, from December 7, 2004 (the opening date of the account) through October 31, 2005, this account received over \$3.1 million in 96 incoming wire transfers from G&SR's Regions Bank account number xxxxxx4851. Also during this time period, over \$3 million was transferred out by G&SR in 2,432 individual checks. A sampling of the checks issued from this account during the first ten days of September, 2005, reveals checks in amounts ranging from \$61.30 to \$90,000, with most checks being in the range of \$100-500. The checks include a notation that "[t]his is a payment on behalf of our mutual customer," and payees are individuals and businesses, including, for example, insurance companies, a law firm, and an internet computer merchant. Accordingly, there is probable cause to believe that this account is being used to fulfill orders placed through OmniPay's bill

payment service, which allows OmniPay/E-Gold customers to order an "outexchange" of E-Gold for payment of a bill whereby OmniPay issues a check on the customer's behalf.

**COUNT I**

29. All allegations contained in paragraphs 1 through 12 are re-alleged and incorporated, herein, by reference.

30. In light of the above-described events, there is reason to believe that the defendant funds were involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1960 of Title 18, United States Code, and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, the United States of America prays that process of warrant issue for the arrest of the defendant funds as described above; that due notice be given to all interested persons to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring the defendant property to be forfeited to that United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court

may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

---

KENNETH L. WAINSTEIN  
United States Attorney  
D.C. Bar No. 451058

---

WILLIAM R. COWDEN  
Assistant United States Attorney  
D.C. Bar No. 426301

---

LAUREL LOOMIS RIMON  
Assistant United States Attorney  
555 4<sup>th</sup> St., NW  
Room 5830  
Washington, D.C. 20530  
(202) 514-7788

**VERIFICATION**

I, Roy Dotson, Special Agent with the United States Secret Service, declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing Complaint for Forfeiture, in rem, is based upon reports and information furnished to me by law enforcement agents and that everything contained therein is true and correct to the best of my knowledge and belief.

Executed on this \_\_\_\_ day of December, 2005.

---

Roy Dotson  
Special Agent  
United States Secret Service

[Whereupon, at 1:50 p.m., the subcommittee was adjourned.]

○